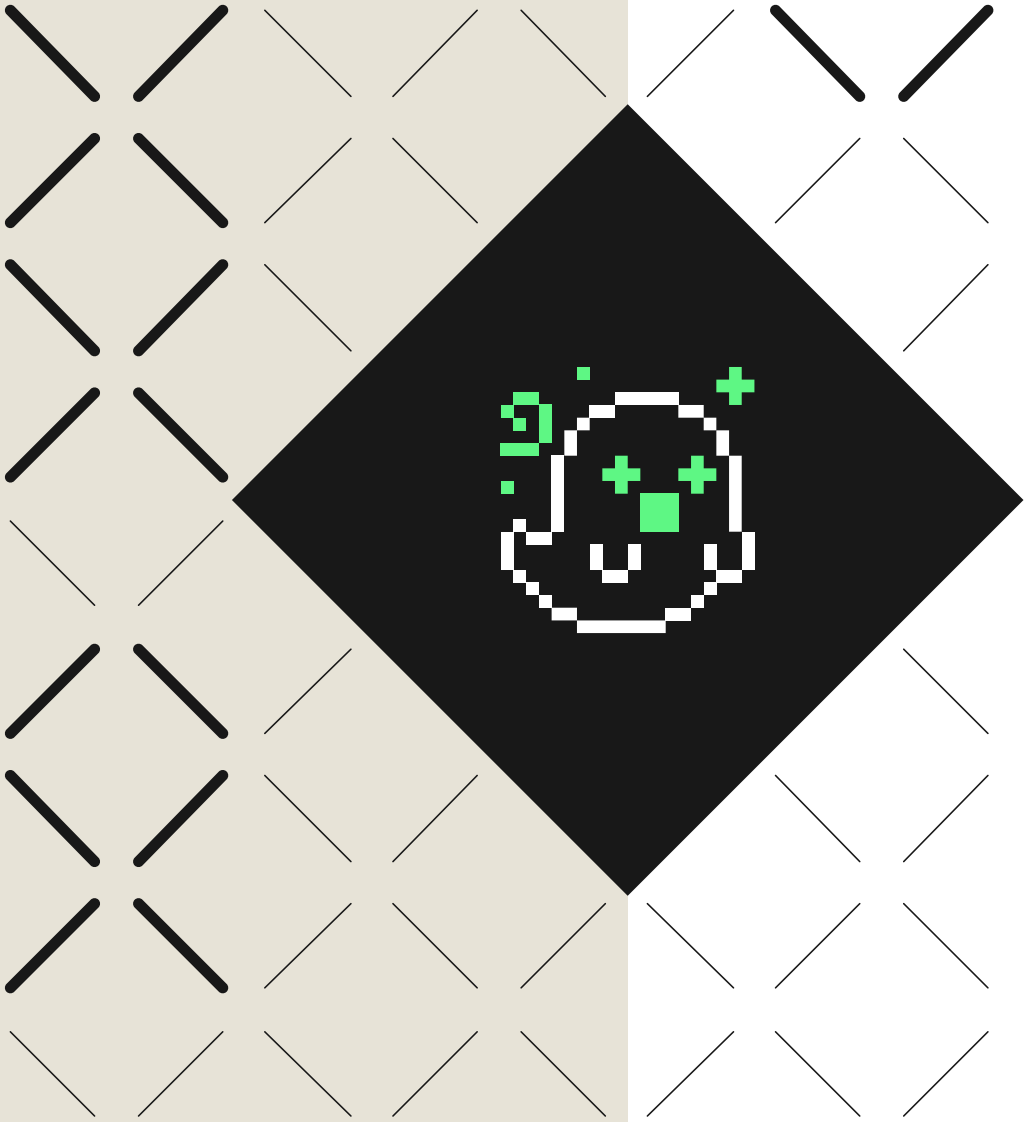


Oh Noes!

INCIDENT MASTER GUIDE

Latest update: July 2026

expel.com

Contents

Introduction 5

- Purpose of incident response prep 5
- The basics of tabletop games 6
- Turning IR tabletops into a game 6

Roles 7

- The Incident Master 7

Creating your character 9

- Attributes 9
- Skills 10
- Modifiers 10

Incident Master guidelines 12

- How to run a scenario 12
- The presentation and scenario sheet 13
- Injects and progressing through the scenario 15
- Effective use of chance 15
- How to involve other people who aren't really there 16
- Awarding XP and leveling up 16

Building your own scenarios 17

- What makes a good scenario 17
- Finding inspiration 18

Ideas on expanding the game 19

- Hit points/leaving the game 19

Playing the red team (adversary mode) 20

- How the sheet inverts 20
- The debrief is the point 21
- A hard line the IM holds 21
- Unfilled seats 21

Two-sided play (blue vs. red, live) 22

- The IM as neutral conduit 22
- Opposed rolls against blue's posture 23
- The action → signal table 23
- Posture worksheet and must-learn-by rails 23

Ending the game and what to do next 24



Welcome to Oh Noes!

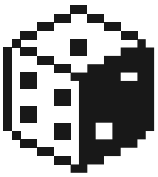
A journey through the cybers and $#*!

Oh Noes! is a game designed to help you and your organization become better prepared to respond to cybersecurity incidents.

This Incident Master (IM) guide is your guide to understanding the game; how to prepare, how to run the game, and how to build on what's here so you can make the game even better.

If you're familiar with Dungeons & Dragons (also known as D&D), you may notice that "Incident Master" is very similar to "Dungeon Master." That's very much on purpose. Oh Noes! is modeled after many great role-playing games like D&D and Stars Without Number. We've tried to make it fun and approachable for people who have never roleplayed, while keeping some of the intrigue and detail that's made games of this type so appealing.

So grab a pencil and your geekiest costume and join us on our journey through the cybers and $#*!.



CHAPTER 01

Introduction

Purpose of incident response prep

When things go wrong at work, it can be stressful. Dealing with technical response, pressures from upper management, incomplete information, and a lack of sleep can lead to bad decisions and bad outcomes.

“But we have an incident response (IR) plan!” you say. That’s a great (and necessary) first step. However, if you’re not stress-testing your plan on a regular basis, you might find yourself struggling to answer questions while trying to respond to the incident at hand. Again, not being familiar with your IR plan in advance leads to bad decisions and bad outcomes.

Clearly, the right answer is to practice your plan. However, in the absence of real incidents, what do you do? Play pretend! Do a tabletop exercise where you pretend a bad thing has happened and you work as a team to resolve the incident. Performed on a regular basis, these tabletops serve two purposes:

- Help identify issues in your organization before real attackers do
- Build muscle memory around the IR process so that when a bad thing happens, everyone knows what to do
- Help to creatively discover areas within your IR plan or security strategy that may benefit from further dicussion and/or gameplay

The more you can tabletop the better. Ideally, you do this once a quarter to keep people fresh and ready for the inevitable—a real incident. Doing a tabletop every three months is far more often than the industry average (we guess more orgs do this once a year, if even that often). But the benefits are incredible when you tabletop quarterly. And when you gamify the tabletop (like with Oh Noes!) people will be excited that it’s tabletop time again.

The basics of tabletop games

A tabletop game is, at its core, a pen-and-paper role-playing experience. There is someone in charge, usually referred to as a "Master" controlling the story and direction of the game. And, of course, there are the rest of the players. Each game is referred to as a campaign. Campaigns can range from simple tales to elaborate and epic adventures, but all include character creation, world building, dice rolls, and most importantly, snacks.

Turning IR tabletops into a game

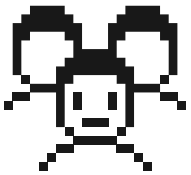
The main purpose of an IR tabletop exercise is to stress test specific parts of your organization and their ability to respond to a bad event. Then, you can take lessons learned from the IR tabletop results to make your organization more resilient and better at responding to future events. Gamifying a process like IR tabletops is a dicey proposition. It's easy for participants to get wrapped up in the game aspect and lose track of what you're really trying to do. While gaming can drive involvement, it can also detract from your stated purpose. Balancing these two competing needs is the key to running a successful scenario in Oh Noes!

Oh Noes! has been designed to strike that balance. While each player creates their own unique character, that character is based on their actual role within the company. For instance, a senior security engineer will still be a senior security engineer in the game, but they can choose to be Balthazar the Destroyer of Firewalls, Senior Security Engineer of the Deep! The player will already have the core skills required to role play as a security engineer, but they can add their own flair.

Similarly, in any given scenario, there are parts of the event you'll want to drive all the players through. If the scenario involves stress testing your organization's response to a successful targeted phishing campaign, you can't leave the success of the phishing up to chance. Rolling the dice to see if the malware executes is not a good idea; the phishing must be successful for you to achieve good results.

Which gets us to a core premise of any IR tabletop: **Don't fight the scenario.**

There will be actions that unfold as part of the scenario that may seem artificial. Or a team member may say, "But that can't happen here." Maybe you do have good controls around mitigating phishing and a successful attack is unlikely. However, testing your response to targeted attacks is important. So, if working through a scenario based around phishing requires a leap of faith on the part of your team to assume an attack was successful, that's okay. If the team accepts that early, they'll better immerse themselves into the game and not worry about whether or not something is technically possible based on their view of the enterprise.



CHAPTER 02

Roles

Like any role-playing game, different people will fulfill different roles in the game. The good news for you is most people will just be playing the roles they normally occupy at work, just with that added flair we mentioned earlier. Let's walk through who does what in Oh Noes!

The Incident Master

The Incident Master (IM) is functionally equivalent to the Dungeon Master (DM) in D&D. The IM controls the execution of the game, provides guidance and help to players, and is the final arbiter of what happens as the game progresses. Simply put, whatever the IM says is what happens.

As the cliche goes, "with great power comes great responsibility." Unlike playing D&D with your friends on a Friday night, if you screw up running a game of Oh Noes!, there are consequences beyond name calling and excessive snacking. Getting a room full of senior people in your organization together for hours at a time represents a real cost to the business, and if the business doesn't benefit from the event, it's really a net loss. You would have been better off not playing. To that end, it's best to understand what makes a good IM and how to prepare yourself for that role.

Skills

A good IM has a broad understanding of the organization they are testing. He or she has a good perspective of the people, process, and technology as well as business motivations and risks the organization faces. The ideal IM has good interpersonal skills and can easily talk to others in the organization. Also, the IM should have a good poker face. As IM, you hold all the cards in the game. Sometimes players go down a road you know will be a dead end, but it's often better to do that and learn rather than correct them. Keeping a straight face will allow you to keep players on the hook longer.

Prerequisites

The IM should be familiar with the company's IR plan, because the scenario will usually (but not always) involve running through your plan. While others in the room may be reading it for the first time (or have totally forgotten what was in it while they claim, "Oh yeah, I totally know what's in our IR plan"), you should know it forwards and backward. Mostly forwards.

The IM should ideally also have some role-playing experience. While this isn't a necessity, it's definitely helpful to understand the basics of role playing, what makes a good DM, and generally how to keep the players on the rails. If you don't have role-playing experience, watching others play on YouTube and Twitch is a reasonable (but not as fun) surrogate to better understand how it works.

Core staff

Beyond the IM, you need players. And the type of players you need depends on what you're trying to test with your IR tabletop. There's generally a continuum of tabletops that range from very high-level and strategic in nature (think: board of directors and senior executives) to others more low level/technical in nature (think: security analysts, system administrators, forensics teams). The type of scenario you run will drive who you invite to participate. If you're doing these events once a quarter, rotate players throughout the year. You can engage senior management one quarter, security operations the next, and engineering the third. The sample scenarios provided with Oh Noes! will give you some ideas on how to engage those groups. As you customize and develop new scenarios, you can better target your organization and its needs.

A quick word on size and scope: try to strike a balance with the number of people in the room and the chaos that can ensue. Too few people in the room and you run the risk of having a very synthetic event where there's too much unknown data and too many untested actions. Too many people in the room and you have 10 sidebars, three people stepping out for calls, and five people who don't understand what's going on or why they're there. In our experience, eight to 10 players is a good size for a game, but let the specifics of your organization drive your decision on size.



Should the IM just be a guide...or a player as well?

In D&D, the Dungeon Master is not usually a player in the game. The DM is a guide and controller and ensures the players have a good time and basically follow the rules while guiding them through an immersive world of their design. The purpose of the IM in Oh Noes! is very similar to that of a DM, but in a corporate environment you may not have the luxury of having a separate person be the IM. For instance, if the CISO is driving the scenario as the IM, you'd want the CISO to actually play the game as well so you can properly model what the CISO would do in the event of an incident. While that's possible, overloading the IM with a player role as well puts extra pressure on the IM. In this situation, the IM needs to be extra prepared so that their IM duties happen naturally and without distracting from the IM's role as a player.

Additional folks and non-playable characters

To play additional people, you may need to create more character sheets to help guide you, the IM, play those additional characters. If you only need the character a handful of times, then you can honestly wing it and use your best judgment. However, if it's going to be a recurring character, then you should create another character sheet. Follow the process for creating a normal character and use that to help play the person.



CHAPTER 03

Creating your character

The character creation process is admittedly a long one, but can be pretty interesting. As you get started with Oh Noes!, here's one important tip: use a pencil. As everyone fills in their character sheets, they'll invariably make mistakes and a pencil eraser will lead to better results than scribbling out screw-ups in pen.

To start creating characters, players must fill in their actual name, position, and character name. Character names should be something fun and unique. If folks are struggling, use this as an icebreaker and make it a group effort. Make sure all characters start at level one with experience points (XP) at zero.

Attributes

Next, you'll guide the players through filling in their five key attributes: RED, BLU, SE, BW, and INT. Beginning with RED, each player will roll three six-sided dice (or one six-sided die three times) and jot down the total of the dice in the first square of the RED row of the dice rolling chart. Do this two more times for RED, recording the total in the second and third square accordingly. Repeat the process for each additional attribute, filling out the grid on the chart. At this point, they must pick one entire column to represent their character. So it's not the best dice roll for each attribute, but the best set of rolls out of the three columns.



Oh Noes! attributes

Like D&D, Oh Noes! characters have attributes that will help (or hurt) their cause as they play through the game. Unlike D&D, Oh Noes! attributes are tailored to the cyber world rather than an imaginary medieval landscape.

RED: Offensive cyber capability. The ability to hack $#*!.

BLU: Defensive cyber capability. The ability to stop people from hacking $#*!.

SE: Social engineering. The ability to get others to bend to your will.

BW: Bandwidth. Your ability to get $#*! done.

INT: Intelligence. Cuz, well, duh.

Here's where it might get confusing, but we'll do our best to explain. Depending on the player's role in the company an attribute may have a "transformer" value. These are defined in Figure 1: Role-specific transformers. For example, the player acting as CEO will have a +1 transformer on the INT, SE, and BW attributes. Instruct your players to fill in the appropriate transformers on the dice rolling chart and then, in the next column, total their chosen dice roll plus any corresponding transformers.

Now, using those totals, have everyone look at the modifiers. Modifiers are specific to ranges in the totals, so for example, if a player has a total of nine for RED, the modifier would be zero. Have everyone record the appropriate modifier in the last column on the dice rolling chart.

Using the information on their dice-rolling charts, players can now fill in the "attributes" section on their player sheet. The number from the "total" column goes in the big square for each attribute, the modifier gets written in the small square.

Skills

Now it's time for skills. Skills are even more personalized to the player's role and personality. Skill levels act as roll modifiers (again, more on that later) and skills can have values ranging from -1 to 2. Each player has three predetermined skills as shown in Figure 1, and can choose three additional skills from the skills section on the player sheet. Have the players write a 0 in the box next to these six skills. All other skills start at -1.

Modifiers

In game play, modifiers change the total of your dice roll. You'll see an example of this in the next section, but all you really need to remember is if you're performing a check against an attribute, add or subtract your modifier from the total of your dice. Use that final value to determine if your check is successful or not.



Using dice

Yes, you just roll them, but it's more complicated than that.

DICE TERMINOLOGY
"3d6" means "three six-sided dice", so "NdX" means you need N amount of an X-sided die.

DICE LEGALITY
When rolling dice, weird things may happen. Dice may fly off the table, land on pencils, and otherwise be disturbed by other objects. If any of these happen, it's up to you as the IM to determine if the roll is valid. As a general rule of thumb, if any of this happens, just reroll to keep the game moving quickly.

WHAT DICE TO USE
Typically a six-sided die is used when your players create their characters and a twenty-sided die is used when you roll for things based on chance. If you're playing a game where you can take damage, you may roll a four or twelve-sided die. Ultimately, it's up to you as the IM to decide which dice you use for each scenario in Oh Noes! It's best to keep it simple unless your players are hardcore role players and bring their own bag of dice to the table.

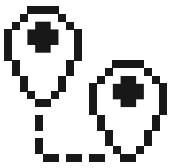
Modifiers

Figure 1: *Role-specific transformers (make additions based on your org)*

Roles	2	1	-1	-2	Skills
CEO		INT SE BW	RED BLU		Leadership, vulgarity, negotiation
COO	BW	INT		SE	Puns, culture, bureaucracy
CTO	RED	INT	SE BLU		Software, puns, innovation
CMO	SE	INT	BW		Puns, culture, negotiation
CISO		INT BLU BW	SE		Leadership, vulgarity, security
IT Lead		RED BLU	SE		Hardware, software, culture
VP Customer Experience	SE		BLU		Puns, negotiation, bureaucracy
Senior Security Engineer	SE	RED BLU	SE		Software, security, innovation

Figure 2: *The modifiers you apply to any roll your character makes*

Dice roll	Modifier (what you change the roll by)
Less than 3	-2
4 - 7	-1
8 - 13	0
14 - 17	1
18 and above	2



CHAPTER 04

Incident Master guidelines

Now that you're finished with character creation, it's time to actually run the game. The first thing to do is pick a scenario. Oh Noes! comes with a handful of pre-built scenarios.

You can use one of those, customize one to suit your needs, or create a brand new one based on your specific preferences. If you choose to make one, there are some guidelines at the end of this guide to help you. For starters, pick an easy one that's aligned with pre-existing concerns and controls you have in place so that you and your team can get familiar with the game play.

How to run a scenario

Scheduling

A game of Oh Noes! can run from two to four hours depending on how complex the scenario is, how many people are involved, and frankly how much fun you're having.

Getting a diverse group of leaders and tech staff in a room for a long period of time can be difficult, so start planning well in advance. Invite everyone and set expectations that they'll spend about three hours with the game.

As you get a better handle on how your tabletops work, modify the time as needed. If the people you're inviting have never done an IR tabletop, you probably want to send them a brief intro about what's going to happen to provide context. Also, if you have an IR plan already, attach a copy to the invite so players can re-familiarize themselves with the plan.

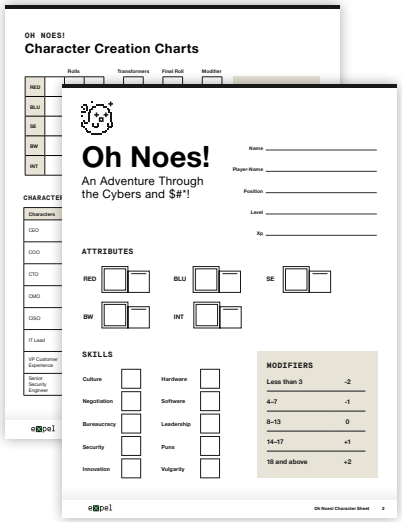
Preparing for the game

Before the event, be sure you're familiar with a few things:

- **Your organization's IR plan:** This event will stress test your IR plan, and it's best to know it as well as you can before you walk into the room.
- **The scenario:** On the surface, scenarios can seem simple; but if you're not prepared, they can tailspin. In particular, know where you can and should use chance to make the game more interesting and unpredictable. That's a skill that will come with time, but knowing the scenario in advance will help a great deal.
- **Your company's security controls:** Or more specifically, the security controls that the scenario will impact. If you're going to do a phishing scenario, for example, you should understand your email architecture, anti-phishing controls in place, what endpoint tech you have, your ability to detect lateral movement, etc.

Before you start

Once everyone is in the room, there are few things to take care of before you start. As part of Oh Noes! we've provided a template presentation to help drive the event itself. So feel free to use those slides to drive the first few minutes of the game.



- **Character creation:** If there's anyone in the room that hasn't played before, have them create their character. Feel free to crowdsource their character's name if they're stuck at "Jeff the Great" as their best option.
- **Process and objectives:** Make sure everyone knows why you're there and how the day will go. Their participation in the post-mortem after the game is just as important as their participation in the game.
- **Ground rules:** There are some guiding principles such as "don't fight the scenario" that you should hit early to avoid getting derailed later. Also, reinforce that there will be no finger pointing or accusation of fault. A tabletop exercise is an opportunity to learn about weaknesses in your organization before they do real harm.

The presentation and scenario sheet

For each scenario, there are two artifacts that you'll be dealing with: the presentation that you show to all the players, and the IM scenario sheet that you keep just to yourself.

The presentation

As the IM, you'll use the presentation to visually drive the game with the players. It contains all the ground rules and objectives as well as all the non-conditional injects. The goal of the presentation isn't to kill people with slides; rather, it's designed to serve as a reminder of what's happening in the scenario right now. If you're not used to role playing, things can get confusing and having a visual reminder is very useful.

In Figure 3, you see an example of a slide in the presentation. For each inject, there's time information (Day 1: Thursday 10:30am) up top. You can use this to drive discussion around staffing and coverage when an event happens. For instance, your company may handle a large malware outbreak very differently on a Monday morning than late Friday night.



Figure 3: *A sample slide from the player-centric presentation*

The presentation also has a step to award XP. XP in Oh Noes! is mostly a matter of pride and doesn't change the game play very much. However, don't underestimate the desire for people to level up and compete over points. In general, you should award points to all players who complete an inject unless someone really screws something up or does an outstanding job. In this case, all players would get 60XP after the discussion for this inject. If a player provides particularly useful insight into CircleCI or a specific exposure you have during this event, feel free to award a few extra points.

The IM scenario sheet

You can see an example of the IM scenario sheet in Figure 4 below. These sheets list the injects, the conditional injects, and more that we'll be explaining in the next section.

Most of this is self explanatory, but it's useful to point out that all of the recommended parties are called out in the spreadsheet. While you may need to tailor this event based on who fulfills what roles in your organizations, this is at least a starting point to get you thinking about who should play the game.

OH NOES!

Incident Master Scenario Sheet

Incident Master	Scenario Name	Who is Present
Bruce Potter	Compromised analyst workstation	CEO, CISO, COO, CTO, CMO, SOC Lead, VP Biz Dev, Security Engineer, IT Lead

Steps	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	SOC catches Cisco Amp alert that suspected malware has been found on an engineers laptop.					Get analyst back online with new laptop		IT lead - Hardware (d6, 3 or better)	• "What endpoint tech do you have? • How can it be leveraged? • Who is responsible for analysis"
2	Infection vector identified as a phishing email spoofed from a penetration tester with a malicious Word doc that purported to contain information about an ongoing incident.	Docx downloaded malware onto the workstation identified that has potential for keylogging, credential harvesting, and lateral movement.	CTO, SOC lead (both try) CYB (d20, 10 or better)		4				• "Who else got the email? • Could our email gateway have caught it? • What extra controls should we put in place?"
3	Night shift online. Endpoint alerts that the two evening shitt SOC analysts laptops are also impacted.	Initial inspection indicates all data on laptops (including VMs) was exfiled to a previously unidentified IP.	CTO, SOC lead (both try) CYB (d20,10 or better)		4				• "What all is on an analyst laptop? • What does an analyst actually have access too? • • How can we turn up auditing?"
4	Inbound customer support request indicates strange activity from account associated with ongoing engagement			All with Pun roll d6 5 or better					• How is our SOC isolated from production penetration testing tools?
5	Customer complains on twitter that our engineers are slow to respond and they are getting annoyed		CMO SE (d20,15 or better) for it to be ignored						• "How do we handle complaints via social media? • How will our customers interpret service degradation? "
6	Further investigation by customer indicates account activity is benign								
7	Cthulhu shows up at the office looking to cause problems. Cthulhu demands great puns or else he's stealing our Digital Ocean creds. Roll for initiative.								• How do we handle our laas credentials?

Notes

expel

Oh Noes! IM Scenario Sheet

Figure 4: *The IM's view of a scenario*

Injects and progressing through the scenario

The primary drivers of the game are injects. Injects are events "injected" into the game to move from one step to the next. They're the core game mechanic and, as IM, you control when they're played and what happens between them.

- **Inject:** This is the action that happens. It requires no skill to learn about, and is the core storyline of the game.
- **Conditional injects:** These are core events too, but you can choose to make people roll for them instead of just giving them that information. The next two columns provide a recommendation on who should roll and what skill or ability they should roll against. Feel free to modify roll requirements based on how benevolent (or malevolent) you're feeling. If you make an inject conditional, and the players aren't successful on their roll, there's usually still a point in the game at which everyone needs to know that information for game play to continue. That's specified in the "Must learn by step" column.
- **Additional objectives:** These are basically "side quests" that you can use to test out additional parts of your organization. While not key to the main story, asking questions like, "How long does it take to get an analyst back online after we've taken their laptop?" can lead to very interesting and useful discussions.
- **Checks:** To determine if a player is able to achieve a conditional inject or an additional objective, have them perform a check. A check is a dice roll where the player has to roll a certain number or better (or sometimes worse) than a set number. The IM view of the scenario has recommendations for each check and who should roll, but feel free to change it to suit your needs.

  IMPORTANT: when a player rolls, be sure to include their modifier in the roll. For example if a player has a -1 modifier on RED, subtract 1 from their roll against RED.
- **Questions:** Sometimes an inject lands and no one is really sure what to do or what to talk about. These questions are seeds for you as the IM to use to try to get dialog going. Also, they can be viewed as notes to yourself to make sure you're covering everything you need to cover.

As the IM, you control the flow of the game. When you've reached what seems like a reasonable end of the discussion after an inject, offer up the next inject. Be sure to give players time to fully explore the impact of an inject before moving along as injects can be an opportunity to learn more about your enterprise.

Effective use of chance

In some role-playing games, it seems like the dice rolls are constant and never ending. Roll for initiative! Roll for damage! Roll to see who gets the chips from the kitchen! The purpose of Oh Noes! is more than just entertainment, it's also to help learn about your organization and make it better. To that end, you can't leave everything up to chance. You must drive players to certain places in the game to test what needs to be tested.

On the opposite end of the spectrum, if you don't leave anything to chance, people are just doing a normal (and potentially boring) IR tabletop. To keep players engaged and wanting to come back quarter after quarter, you have to facilitate some chance acts. If you've never played a role-playing game before, recognizing how and when to include chance can be a daunting task. If you've never played, you may wish to consult someone in your company that has and have them join the game for the first few rounds, just to guide you through the process.

With the sample scenarios, we've listed some places and circumstances where chance is appropriate. Feel free to modify our recommendations based on the people who are attending the game. Over time, you'll get to know the game and it will become easier to manage chance in the game play.

How to involve other people who aren't really there

At some point in the game, you'll get to a point where there's a question on the table that no one in the room can answer. You have a few options available at that point:

- **Call a lifeline:** You can call or otherwise reach out to the person who does know and get the answer. The danger is you may completely derail the conversation because you have to bring the person up to speed and then get the answer to your question while basically everyone in the room sits and waits.
- **Make an executive decision:** Using your best judgment, you can just make up the answer. While you may be incorrect at least you can keep the game moving forward. The danger here is that a wrong answer may not allow you to properly test the controls in your organization.

It's useful to reach out to people who may be lifelines in advance of the game to prepare them about the scenario and the types of questions that may come up. This limits the risks of calling them and keeps the game moving as quickly as possible. Just be sure to swear them to secrecy in advance to make sure they don't leak info on the scenario to the players.

Awarding XP and leveling up

The XP in Oh Noes! don't matter for anything except pride and bragging rights. That said, pride and bragging rights are what will keep people coming back for more games. It's important to give out points at the end of the game and have players track their points as part of their character.

In the early levels, there should be enough points in each scenario that a player should level every time they play. There are exceptions that you can use as an IM; for example, if someone has to step out to take a call for a few injects, you can withhold the points while the person is gone. You can also choose to award extra points for those who really did an outstanding job. You can even award skill points if people show a propensity for a certain skill. As an IM, you have total control over the game, and just like Drew Carey in "Whose Line Is It Anyway?" the points don't matter so have fun with them.

Level	Total XP
1	0
2	100
3	225
4	375
5	550
6	750



CHAPTER 05

Building your own scenarios

Oh Noes! comes with canned scenarios that you can use to drive your tabletop games. However, like its role-playing game counterparts, this game is designed for you to make your own. By customizing it to your own needs and the specifics of your enterprise, you can make Oh Noes! more relevant and engaging to your coworkers and company.

What makes a good scenario

Here are a few tips that, in our experience, help make for good scenarios.

- **Keep it simple:** This cuts several different ways. First, don't create overly complex situations. There are a lot of players in the room and even simple scenarios have a way of taking up allotted time. Plus, don't underestimate the players' ability to take a scenario in a direction you don't anticipate. Leaving out some details helps you drive to new places in the situation you hadn't planned on.
- **Attack one problem:** In the same vein, if you're trying to stress test your response to a targeted phishing campaign, just do that. Don't also test your ability to respond to a literal fire as well. This will keep your after-actions more targeted and more detailed.
- **Don't do impossible things:** While people should "trust the scenario," you shouldn't do things that are completely impossible. Hacking through the firewall is not something that makes any sense, so don't integrate something nonsensical like that into your scenario. Find a different way to test the thing you're trying to test.

Finding inspiration

There are lots of ways to get ideas on new scenarios to implement. We've all had bad days at work that would make good table top events. But if you're stuck for ideas, check out the @badthingsdaily Twitter account (https://twitter.com/badthingsdaily). There are hundreds (thousands?) of ideas on that account and links to other places to get inspiration for tabletop scenarios. Between your own bad experiences and tweets from @badthingsdaily, you should have a never ending list of things to turn into scenarios.



CHAPTER 06

Ideas on expanding the game

We designed Oh Noes! so you can customize it to your needs. Beyond custom scenarios, there's lots of game play elements you can add. Depending on your audience, their technical chops and interest level in role playing, you can start to draw in elements from other role-playing games to make things even more engaging.

Hit points/leaving the game

Hit points (HP) are another very common metric for tracking progress in a game. But unlike XP which increases with achievements, HP goes down, and once you're out of HP, you're typically out of the game. That's problematic because in real life, you usually don't have people passing out on the floor in the middle of an incident. One would be strange, but having most of your players knocked out is downright horror movie material.

You could consider something where you take HP for people missing rolls or other mistakes and the first person to zero is knocked out of the game. Once the first person is knocked out, no one else can be knocked out for the rest of the scenario. We call this the "family emergency" where a player has to leave work due to a sick family member. There are other ways to try to implement hit points, however. Feel free to experiment and extend the game in a way that works for you.



CHAPTER 07

Playing the red team (adversary mode)

A red team session is a separate sitting where the whole table plays the operator crew instead of the defenders. It runs on the same sheet mechanics you already know—injects, checks, questions, an IM answer key—but the lens is flipped.

How the sheet inverts

- **The Inject is the friction the crew must survive:** The SOC noticing, a failed-logon spike, a credential reset, law enforcement making contact. What was the defender's win is now the operator's obstacle.
- **The Questions are operator strategy:** OPSEC, monetization, when to cash out, weighing noise against payoff. They stay at the level of *decisions, economics, and psychology*.
- **The Checks are RED-primary:** The crew rolls to pull off a move against the environment, using the adversary roles below.
- **The answer key reads SHARP/SLOPPY/BURNED**: The disciplined, economically rational play; the one that works but wastes money, time, or noise; and the greedy, loud, or premature move that gets you caught.

The debrief is the point

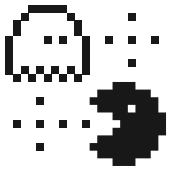
Every red team step carries a **defender's mirror**—the blue-team lesson that operator move just taught. Run the session for the crew's decisions, then close on the mirrors: thinking through the attacker's economics shows a defender exactly where their defense is cheap and high-leverage. If a step can't be mirrored into a defensive takeaway, cut it.

A hard line the IM holds

Red team play is a strategy exercise, not a how-to. It never provides operational uplift—no exploit specifics, tooling-as-instruction, command sequences, or working phishing or malware detail. Keep every operator move at the decision and effect level. If the table drifts toward real technique, steer it back to the economics; the decision-level framing already teaches everything a tabletop needs.

Unfilled seats

The IM plays any unfilled operator seat as an NPC, making the **minimal competent move** that keeps the intrusion chain (access → operate → infrastructure → monetize) continuous, not the cleverest possible play. A missing seat never stalls the scenario.



CHAPTER 08

Two-sided play (blue vs. red, live)

Two-sided play runs a blue scenario and its red twin at the same table, at the same time. The blue team works the incident under the IM as normal; one or more **red players** run the operator crew. Neither side sees the other's plan. Like Battleship, each learns about the other only through observable outcomes.

The IM as neutral conduit

The IM has **know-to-adjudicate** knowledge, not **know-to-coach** knowledge. The IM must see each red action the moment it's declared—someone has to set the target and resolve the roll—but relays to blue only the observable signal the outcome produced, and nothing about red's intent, plan, or the dice. The IM strategizes for no one, hints to no one, and keeps a poker face. If you wouldn't tip a player toward a dead end in classic play, you don't tip either eam here.

The turn loop

- **Red declares—**each seat privately declares one action from its playbook (the IM covers unfilled seats).
- **IM sets the target** from blue's current posture on the vector the action touches.
- **Red rolls** d20 + the role's modifier; the IM reads the outcome band.
- **IM relays the signal—**the pre-written, blue-observable inject for that outcome, and nothing more.
- **Blue responds**, and their actions **update the posture**: hardening a vector raises Red's future targets there and can close a foothold entirely.

Opposed rolls against blue's posture

Red rolls against a target derived from how well blue has hardened the vector in play. Where blue neglected it, the shot is easy; where they hardened and preempted, it's brutal—and a near-miss on a hardened vector tends to generate the *louder* signal, because good defense turns attempts into detections.

Blue posture on the vector target (d20 + mod)	Target (d20 + mod)
Neglected/unaddressed	**6+**
Basic control present	**11+**
Hardened/actively monitored	**15+**
Hardened AND blue preempted this game	**18+**

Outcome bands: beat by 5+ or a natural 20—full success, minimal signal; meet the target—success that produces an observable signal blue can catch; miss by 1–4—partial effect and a louder artifact; miss by 5+ or a natural 1—no effect and a clear detection.

The action → signal table

Improvising "what would blue see?" under pressure is where a live two-hander breaks down, so each Two-sided scenario ships an **IM-ONLY** table mapping every operator action to the blue-facing inject at each outcome band. Signals describe only what blue's tooling and people would surface—never how the action was performed. That is both the mechanic and the safety boundary.

Posture worksheet and must-learn-by rails

The IM keeps a private posture worksheet—vectors such as initial access, endpoint, identity, lateral movement, exfil, comms, and backups—each at a level blue raises through play. And because a live game can diverge, each scenario lists a few must-learn-by beats: if red's path hasn't surfaced a key lesson by its step, the IM injects it directly so the scenario still teaches.

A note on the expanded character system

Two new blue roles (SOC Lead, Engineering Lead) and five adversary roles now appear on the Character Sheet. Every role uses the same five attributes and the same ten skills as the base game—the new rows only tilt each seat toward its part of the work. See the 2026 Character Sheet update for the transformer values.



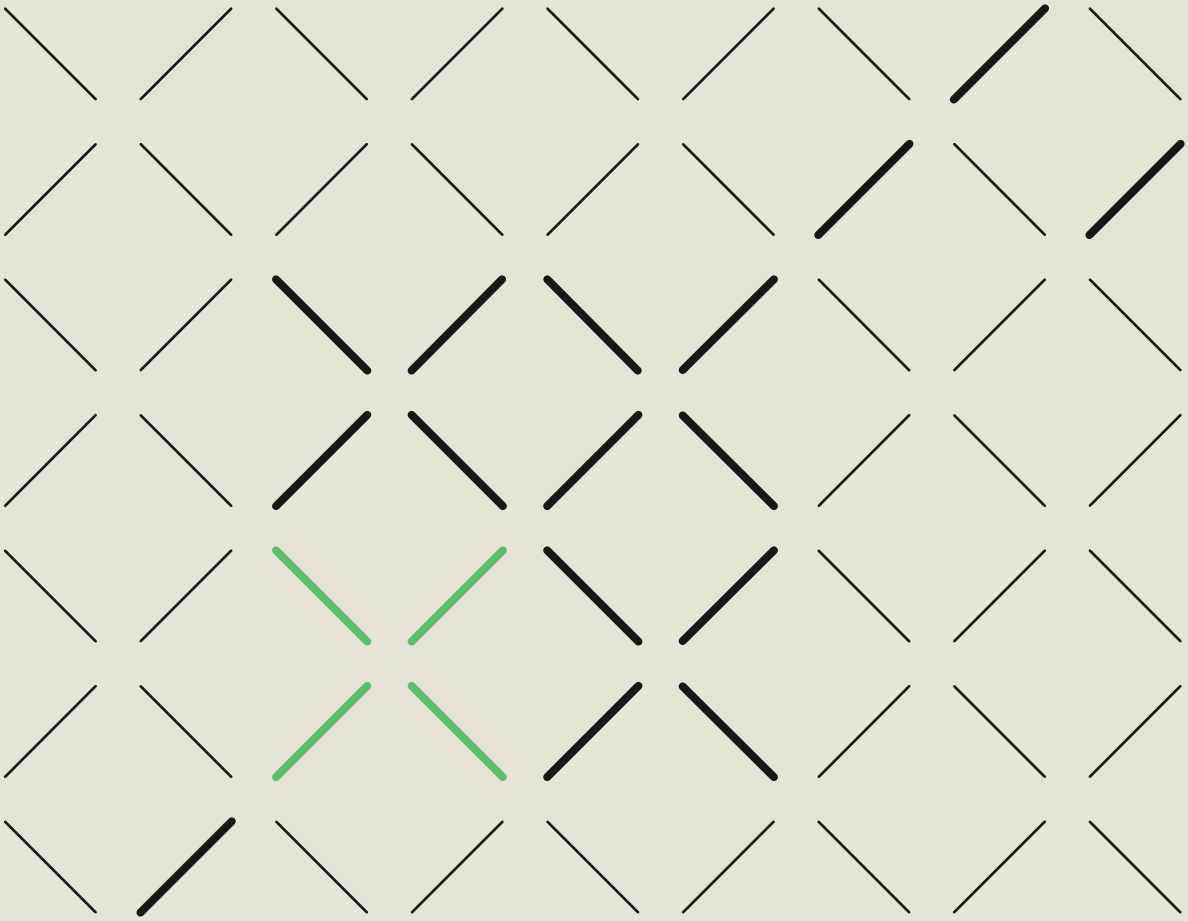
CHAPTER 09

Ending the game and what to do next

As the IM, you'll declare the game over once the scenario is complete and the threat is mitigated. At that point, have players calculate their XP and apply it to their character sheets. Keep those sheets in a safe place—or have your players save them—so they're handy for the next time you play Oh Noes!

And while completing the mission is rewarding and useful, so is looking back on the overall quest and evaluating the different steps, achievements, mistakes, and opportunities. Schedule a post-mortem to review how the exercise went. Give it at least a few days so that all the players have a chance to think back on the experience, but not so long that they forget the important details. Then apply those lessons learned to improve your results for the next time you play Oh Noes!

And that's it! We hope you enjoyed your time playing Oh Noes! and that you use it for your regular IR tabletop exercises.



License

Oh Noes! Is licensed under Creative Commons Attribution. See https://creativecommons.org/licenses/by/4.0/ for more details. Ultimately, we want people to use, modify, and generally make Oh Noes! a game that helps make organizations better prepared to deal with incidents. The Attribution license is the most open of the Creative Common Licenses and we hope that others will feel free to build on the work here.

Authors

Bruce Potter and Robert Potter created the original Oh Noes! version and first presented it at DefCon 2018 in Las Vegas. Red team gameplay mechanic and scenarios added by David Johnson. The Expel team updated Oh Noes! in 2026.