



National Cyber
Security Centre

PART OF
THE GCSB

Rolls & Responders

Game Manual

Rolls and Responders is licensed under the Creative Commons Attribution 4.0 New Zealand licence, available at www.creativecommons.org/licenses/by/4.0/.

This page is intentionally left blank.

Licensing and Acknowledgements

Rolls & Responders is licensed under the Creative Commons Attribution 4.0 New Zealand licence, available at www.creativecommons.org/licenses/by/4.0/.



You are free to copy, distribute, and adapt the work, so long as you attribute the work and abide by any other licence terms. For the avoidance of doubt, this means this licence applies only to material as set out in this work.

Special thanks to Kate Pearce and TradeMe New Zealand for sharing the original concept through the NZITF, as well as their helpful feedback throughout the development process.

Contents

| | |
|----------------------------|-----------|
| Introduction | 5 |
| Getting Started | 6 |
| Game requirements | 6 |
| Setup | 6 |
| Gameplay | 6 |
| Resolving actions | 8 |
| Advantage and disadvantage | 9 |
| How time works | 9 |
| Facilitator | 10 |
| Glossary | 12 |

Introduction

Welcome to *Rolls & Responders*, an open-source tabletop exercise toolkit for cyber security incident response teams.

Rolls & Responders (R&R) is a dice-based role-playing game (RPG), in which players assume the role of themselves or other characters that perform actions in a fictional setting.

In the context of *Rolls & Responders*, the players respond to cybersecurity incidents. They do this by following their organisations incident response plan, discussing their thoughts and making a series of structured decisions with consequential outcomes.

The system uses two dice to determine events within the game; one is used to randomise the scenario at the start of the game, while another is used to determine whether participants are successful when performing actions.

There are no complex rules for players to learn, making *R&R* a quick exercise to set up and play, while providing an engaging toolkit for structuring critical discussion and aggregating incident response knowledge.

Tabletop exercises are a simple format for practicing and stress-testing incident response plans. Participants are presented with a hypothetical scenario where they will take turns discussing how they would respond over the lifecycle of the event.

The goal is to manage the scenario as effectively as possible, while building familiarity with their existing business frameworks.

In doing so, this exercise will highlight any potential gaps in knowledge, procedures, and capabilities.

During a debrief, the scenario and outcomes are evaluated after the exercise where the facilitator and the group will then discuss what went well and what could be improved.

These tabletop sessions are guided by a facilitator. The facilitator is anyone who volunteers or that you elect to play the guiding role in *R&R*.

Facilitators offer injects and formalising the outcomes of player actions. The facilitator may also receive support from subject-matter experts, who are able to provide insights into specific features of the scenario that some players may be unfamiliar with. The facilitators are valuable to the debrief process, as they can evaluate the discussion and effectiveness of the response.

Rolls & Responders includes a quick guide for participants and facilitators, a detailed manual for Facilitators, and a set of pre-constructed scenarios with various levels of difficulty so that players can get started right away.

R&R also features a set of tables for generating injects and scenarios, enabling teams to write bespoke incidents to fit their business needs or randomise the scenarios so that no two sessions are the same.

Getting started

Game requirements:

- 1 x six-sided die (D6)
- 1 x twenty-sided die (D20)
- A table in an isolated space with no distractions
- Scratch paper or whiteboard for planning and note taking
- Your organisation's incident response plan

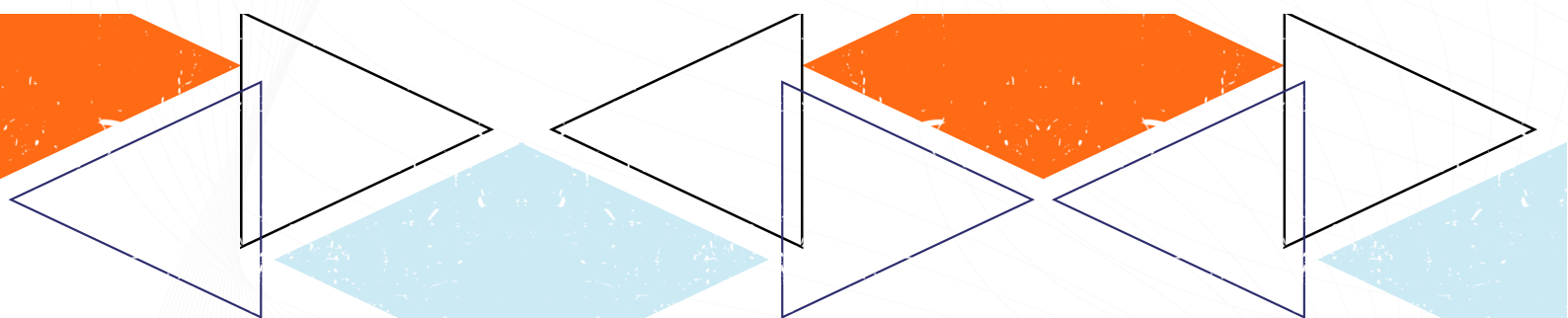
Setup:

The Facilitator first chooses a scenario. This can be one of the pre-constructed events which can be found in a supporting document, or a new scenario can be constructed by rolling a six-sided dice four times using the scenario generator; each roll decides a different feature of the event, which the Facilitator notes down before play.

Participants should prepare by familiarising themselves with their organisation's incident response plan and the roles and responsibilities listed in that plan. Players can choose to take on roles from the incident response plan in advance, or they can be decided as the game develops.

Gameplay:

A game of *Rolls & Responders* takes place over three turns. Each turn representing different stages of response to the challenges presented by the incident.



Turn 1: Pre-Incident

The Facilitator sets the scene, providing information and corresponding challenges of the scenario. Based on information provided by the Facilitator of the scenario, the responding players are likely to already understand how they would choose to respond as the scenario evolves.

Players make early decisions around whether to declare an incident, what roles each player will assume from the incident response plan, what further information they need to seek out, what actions members will need to take, and what resources they may require. This turn ends when the players declare an incident.

Turn 2: Response

The Facilitator announces updates about how the incident is progressing and the results of any actions the players have taken. The Facilitator may deliver a randomised inject. Injects are specific events or actions that take place within the scenario.

The Facilitator plays injects within the game to simulate real-world events. Game participants are expected to respond to the inject.

Players organise their response, designate tasks and manage their resources. This turn ends when the players have learned enough about the incident to decide on a course of action to begin recovery.

Turn 3: Recovery

The purpose of this turn is for players to discuss the recovery and longer-term implications of the incident. The Facilitator outlines what has happened during the intermediary period since the last turn.

Players discuss the tasks that still need to be performed and assign work to address them.

After this, the game ends. The participants should make time to engage in a debrief, but if this is not possible, a similar meeting should be held later to discuss insights.

Note:

At the end of each turn the Facilitator may choose to have a short break to plan updates and injects for the next turn.

Gameplay then resumes, with the Facilitator announcing what has happened and opening the floor for players to plan their next round of actions. Turns can cover longer periods of time if the room agrees that certain actions will take longer to properly take place.

Resolving actions:

Rolls & Responders uses a combination of dice-based and consensus-based solutions. This means that the difficulty of a given task is decided in conversation between the players and the Facilitator. This helps to ensure accuracy, while success or failure still contains an element of chance to simulate the uncertainties and variables of real life.

The result of a six-sided die is used to determine events within the scenario. This includes generating the scenario itself, as well as the occurrence of injects – random events that can add difficulty or complexity to the response from the players.

The Facilitator is the only person that uses the D6.

The twenty-sided die is used for resolving Player actions. When performing a task, the participants discuss how difficult it would be to perform. This decides how high a Player needs to roll to successfully complete the task.

The Facilitator usually has information about the incident that the players do not have, and therefore the Facilitator always has the final input.

When participants have agreed on an action, the facilitator should track how long that action should take.

This will allow the facilitator to move the game clock forward and means players must divide work accordingly amongst themselves.

| Difficulty | Example | Minimum Required roll |
|--------------|---|-------------------------------------|
| Trivial | Checking your inbox | No roll required (still takes time) |
| Routine | Examining logfiles | 5 |
| Challenging | Using an unfamiliar tool | 10 |
| Hard | Extracting malware source code | 15 |
| Elite Hacker | Highly complex and inspired feats of technical wizardry | 20 |

To succeed on a challenging roll, the player must roll a 10 or higher on the die.

A successful roll means the action is completed by the next turn. The Facilitator may choose to reveal information the player might have uncovered, or otherwise describe the outcome of the dice roll.

An unsuccessful roll means the task is not completed and must either be re-attempted on the next turn, or an alternate solution found.

The Facilitator can decide the consequence for a failed roll, such as the failed action taking additional time, a system shutting down temporarily, or negative press coverage – adding pressure to the team.

Advantage and disadvantage:

Sometimes, extra factors within the scenario may further impact a player's likelihood of success. To reflect this, the Facilitator can choose to have players roll with either advantage or disadvantage. To do this, the player must roll two dice and use the higher value (advantage) or the lower value (disadvantage).

An example of advantage might be if one player helps another – such as by taking time to supervise them on something particularly challenging. The player performing the action rolls two dice and uses the higher value (if any).

Disadvantage works the opposite way. For example, if a responder has fatigue from working late into the night, the Facilitator may require them to roll twice and use the lower value (if any).

Advantage and disadvantage occurring simultaneously will cancel each other out, so the player rolls a single die as normal.

How time works:

There are only so many hours in the day, and responders must often work against the clock to ensure their business resumes function.

In *Rolls & Responders*, teams need to consider how they will manage their time over the lifecycle of an event.

This can include:

- Which team members are rostered on at any given time;
- The hours they can devote to the response alongside their normal workload;
- How long individual tasks will take;
- Whether additional hours need to be allocated; (e.g. a staff member may stay late in the office to complete a task)
- The amount of flexibility with certain deadlines (notifying stakeholders, etc).

Players should discuss these factors when planning the team's moves each turn, so they ensure tasks are prioritised effectively.

As noted in the section on rolling with advantage/disadvantage, overstressing team members can also impact performance and outcomes.

Facilitator

The Facilitator creates the session and sets the scene. They announce events during play, and guide discussion prompted by the scenario.

A good facilitator drives the narrative and cadence of the game, and they ask thoughtful questions to inspire and prompt thoughtful responses from players during the incident response process.

We recommend the facilitator sets up the scenario in advance by rolling the six-sided dice four times to generate the scenario.

This will allow you to develop a short back story and think about what prompts and injects you might want to give to your players. You do not need to spend long on this task.

When facilitating, it is helpful to be familiar with the issues and organisations involved, but it can also be useful to have a subject-matter expert or a similar person to consult when determining injects and resolving actions.

The Facilitator may want to have a subject matter expert or similar person to consult with when determining injects and resolving actions.

For distributed games, which take place online when players are offsite, or with multiple teams involved, the Facilitator should consider including a technician within their team.

This person will be responsible for operating the software, monitoring breakout rooms and group chats, and timekeeping. This frees up the Facilitator to concentrate on the game and the participants.

The quality of discussion and learning heavily depends on aggregating the knowledge and experience of all participants. A core responsibility for Facilitators is ensuring all players can share their insights and ideas, so they should endeavour to make the game a space where everyone feels safe, respected, able to speak, and is allowed to make mistakes.

Establishing ground rules for the conversation is useful, as well as a method for participants to discreetly contact the Facilitator in the event of any issues.

It's important to ensure that participants are aware the game is not a test or a competition where the goal is to win. It is primarily a knowledge-building exercise designed to test and improve your incident response plan.

The Facilitation team is also crucial to the debriefing process. Ask the participants to consider what worked well, where gaps may exist in their processes, and which insights they will carry forward into any future exercises.

The Facilitator may also like to devote a small amount of time to discussing their observations about how the game itself ran: how the conversation flowed, if there were any procedural or technical difficulties, and how effective it was as a learning experience.

This feedback is useful for improving future sessions, developing facilitation skills, and designing other types of exercise.

Remember that *Rolls & Responders* is a tabletop exercise, not a full simulation. The focus is on systems and decision-making. This takes work off both you and the players, as the events are externalised through theoretical decision making.

Comprehensive pre-written inject materials, such as mock-social media posts and logfiles, are not necessary but can help immerse players if you have the time to produce them beforehand.

Providing basic information about the scenario as it unfolds, which the team is likely to know at a given point, should usually be enough.



Report an incident

For more information, or to report a cyber security incident, contact us:

ncsc.govt.nz/incidents

Glossary

| | |
|--------------------|--|
| Inject | An unexpected event or action the Facilitator injects into the players turns to simulate a real-world scenario. |
| Tabletop | A tabletop exercise is an informal, discussion-based session in which a team of players discuss their roles and responses to predetermined scenarios during an event. |
| Facilitator | The Facilitator drives the narrative and cadence of the event. They influence the groups decision making ability by furthering the event through a series of prompts and in inspiring questions. |
| Player | A participant in <i>Rolls & Responders</i> that assumes any role and responsibilities as agreed by the team. |
| D6 | A six-sided die. This is used by the facilitator to set up the game, and to provide details for some of the injects. |
| D20 | A twenty-sided die. This is used by the players to set up the game, and to provide details for some of the injects. |

This page is intentionally left blank.



**National Cyber
Security Centre**



*PART OF
THE GCSB*