Manual and script for organising cyber crisis exercises

based on Cyber Crisis Exercise OZON

Utrecht, April 2017

Credits

Manual and script for organising cyber crisis exercises
based on Cyber Crisis Exercise OZON

SURF
PO Box 19035
NL-3501 DA Utrecht
Tel. +31 88 787 30 00

info@surf.nl
www.surf.nl

April 2017

SURF is the collaborative ICT organisation for higher education and research in the Netherlands.
This publication is available in digital format on the SURF website: www.surf.nl/publicaties

Table of Contents

1. Introduction

In October 2016, SURF organised a major two-day cyber crisis exercise called OZON. In all, some 200 participants from 28 institutions took part in the exercise. The OZON Cyber Crisis Exercise proved to be a successful first simulation exercise. The institutions and players participated actively and enthusiastically. The exercise received an extremely high rating, both in terms of its content and the achievement of its objectives.

The OZON Cyber Crisis Exercise has been a gap-bridging exercise, building bridges between management and communication and ICT departments, both internally and between the institutions. The different levels within the institutions – management, communication and ICT departments – communicated well with each other. It was often the first time they had done so in relation to a cyber crisis. There was also a good deal of communication between the institutions themselves. The functioning of the system and the effectiveness of crisis communications were reviewed.

The participants recognised the importance of the exercise in raising awareness. The players found the scenario extremely realistic, fun and highly instructive. Some institutions continued playing beyond the official end of day one, and everyone was keen to resume proceedings on day two. Some managers asked if they could participate in the exercise for longer than they had intended. OZON has prompted many institutions to give greater consideration to the issue of cyber security.

Preparation of the exercise was an intensive and time-consuming process. And the exercise also proved more difficult than expected for the players. Given the impact of the exercise, however, the effort was worthwhile. Cyber security is now on the agenda, there is greater knowledge and awareness around the issue, and bridges have been built between the tactical/operational level and the strategic level, both within and between institutions.

Many of those who took part in the exercise said they would like to see more of these exercises taking place, on both a large and a small scale. It is for this target group that we have produced this guidance, which is based on the OZON exercise.

This guidance and plan for cyber crisis exercises can be used to organise both large-scale and small-scale cyber exercises, and is intended for (ICT and) security specialists. These exercises can be organised both within individual institutions and between institutions or even at sector-wide level.

Document structure
Chapter 2 discusses the planning of a cyber crisis exercise based on the preparation, execution and evaluation phases. Chapter 3 describes the roles, tasks and actions, and the form they take during the preparation phase and during execution and evaluation of the exercise. Chapter 4 outlines the internal tasks, resources and materials needed to set up the scenario and keep participants informed as well as the documents required during the exercise itself. The various communication media are also discussed. Chapter 5 considers the logistical aspects of the exercise. Chapter 6 explains how to organise a Capture the Flag exercise (optional). Chapter 7 considers the evaluation process, including the specific evaluation points, evaluation of the exercise process itself and evaluation of the crisis management structures.

Finally, the appendices include a detailed schedule, a checklist, details of the different types of exercises that are possible, examples of a scenario and other information that may be useful when planning and implementing a cyber crisis exercise.

For more background information on risk management and crisis management, general background information on developing a cyber crisis exercise and the lessons learned from the OZON Cyber Crisis Exercise, please refer to the 'OZON Cyber Crisis Exercise White Paper, a gap-bridging exercise'.[1]

[1] https://www.surf.nl/en/knowledge-base/2016/whitepaper-cyber-crisis-exercise-ozon.html (checked 01 July 2017)

2. Planning a cyber crisis exercise: preparation, exercise and evaluation

2.1. Planning – the basic principles

A simulation exercise on the scale of OZON requires a minimum of six months' preparation. Preparation time, holidays, number of meetings, execution and evaluation must all be taken into account in this context.

The time required to plan the exercise will depend on the complexity (operational/tactical/strategic) and scope of the exercise and on the available resources. If the exercise involves multiple institutions participating simultaneously, the institutions will have to apply to take part. Decision-making regarding participation at management level and large-scale participation takes time, particularly where management itself is to be involved. It is important to take this into account in the application process.

In the case of OZON, the deadline for applications was initially set at 27 April. However, given the high level of interest, we had to close the registration early. As a result a number of participants that had not yet taken a decision were not able to participate at the desired level. If an event takes place on an annual basis, this should be taken into account in the annual plan.

Where a large number of institutions are involved in the exercise, it is helpful to set meeting times in advance. Devising and developing the scenario is the most time-consuming part of the process.

The planning process must consider the following:
- date and time of the exercise;
- duration of the exercise;
- availability of key players;
- other events, in order to avoid clashes with the intended execution date;
- decision-making process;
- holiday periods;
- preparation of the scenario;
- preparation of the technical and strategic evidence for the scenario;
- inviting, informing and briefing participants;
- evaluation.

See [Appendix 5: Planning timeline for OZON 2016] for a graphical timeline including dates, deadlines, action points and meetings, as used in the OZON Cyber Crisis Exercise.

2.2. Timeline/plan for the organisation of a cyber crisis exercise

Record actions, activities, deadlines and meeting times in a timeline/plan. Also indicate who is responsible for what.

Tasks that must be taken into consideration include:
- establish client, create budget and generate support;
- set up project group;
- define objectives, needs and nice to have list and type of exercise;
- decide on location of exercise and logistics such as lunch;
- schedule meetings of project group, programme group and steering group;
- decide on a name;
- define and document communication media;
- send out invitations to participating institutions;

- deadlines for registration;
- decide on dates and content of evaluation(s);
- write scenario, both central and institution-specific scenarios;
- decide whether you will use a media simulator and, if so, which;
- devise and document communication plan;
- draw up a schedule for the exercise itself;
- draw up a schedule for the logistical aspects of the exercise;
- generate support within the institutions;
- produce documentation for players;
- player briefing;
- design, develop and roll out technical elements;
- create interventions;
- where appropriate, invite external parties to participate in the exercise and explain to them what the exercise involves;
- assess and review evaluation;
- communicate results within the institution(s);
- when setting up a bronze exercise also: brief and instruct infiltrators and provide them with proof of exemption.

A sample plan/timeline from the OZON Cyber Crisis Exercise is available in [Appendix 6: Sample timeline for organisation of OZON Cyber Crisis Exercise] and a sample checklist in [Appendix 18: Checklist for organising a crisis exercise]. The roles and tasks involved are explained in detail below. You can find examples in the appendices.

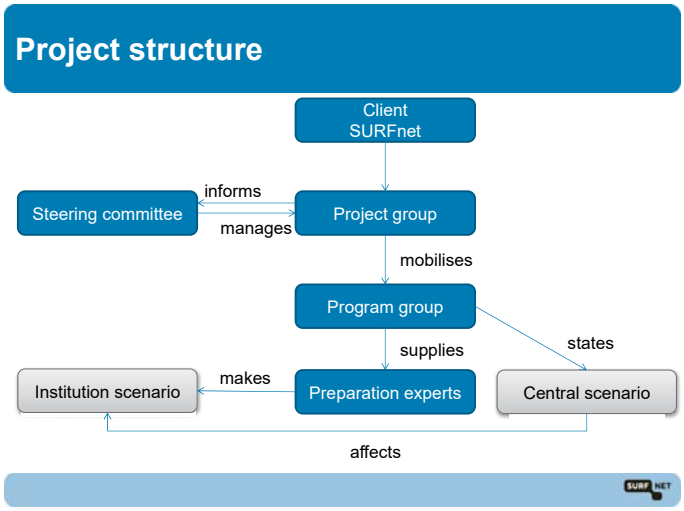
2.3. Prerequisites

When organising the exercise, keep the following aspects in mind:
- impact on operational processes and infrastructure;
- role of security officers;
- role of the preparation team;
- criteria for interrupting the game; and
- ensuring that the game remains within a closed environment.

For more detailed information on this, see [Appendix 4: Prerequisites for the success of the exercise].

3. Roles, tasks and actions

3.1. Prior to exercise



3.1.1. Client

The client makes time, money and manpower available to enable the crisis exercise to take place.

3.1.2. Project group

Set up a team that consists of a project manager, project secretary, communications officer and project members.[2] The project team is responsible for the scenario (both strategic and technical), the documentation, the logistics of the exercise and the evaluation.[3] The sub-topics can be prepared by individual project members and/or within the project group.

The project group should include the following roles (the same person may fulfil several roles):

- The **project manager** is responsible for the planning and execution of the exercise. For a two-day exercise, the role of the project manager entails an effort of approximately 15 days.
- The **project secretary** takes the meeting minutes, is responsible for setting up an information platform (e.g. a wiki) and sends all central communications to the steering group, project group and programme group. For a two-day exercise, you should allow for approximately 20 days for the project secretary.
- The **communications adviser** devises and rolls out the internal and external communications strategy. Where appropriate, this will be documented in a communication plan. For a two-day exercise, the role of communications adviser entails an effort of approximately five days. See [Appendix 13: Content of a communication plan].
- The **exercise leader** leads the exercise and stays in contact with the project manager and the central exercise team/response cell. This role can also be taken by the project manager. The exercise leader must have experience with crisis exercises and be able to improvise. For a two-day exercise, you should allow for five days for the role of exercise leader. (Preparation and supervision of exercise).

2 ISO 22398:2013(E), Art. 5.2.4.1, p. 10
3 ISO 22398:2013(E), Art. 5.2.1, p. 8

- **Project members** take on a variety of (optional) tasks:
    - **Technical preparation of the scenario -** For a two-day exercise, you need 24 days for technical preparations. See [Appendix 10: Technical elements of scenario].
    - **Creation of central scenario** – For a two-day exercise, you need two days. See [Appendix 7: Creating a scenario for a simulation exercise].
    - **Supervision of creation of institution-specific scenarios** – For a two-day exercise, plan 40 days for supervision of inexperienced exercise planners who are devising institution-specific scenarios (in 28 institutions, of which 14 are Gold/Silver and 14 Bronze).
    - For a two-day exercise, plan 45 days for **organisational and advisory tasks** (e.g. project management, stakeholder management, procurement of resources, facilitating events, meetings and exercise, setting up and maintaining a wiki, facilitating exercise days, leading the exercise days, logistics, and organising, planning and leading the (joint) evaluation sessions. This will be discussed in more detail later in this guide.)
    - **Optional:** Organising **joint work sessions/workshops** helps develop the expertise of the preparation team. The exercise planners can work on the scenarios together, share their experiences and broaden their knowledge. It also allows the scenarios to be coordinated with each other (when this is one of the objectives of the exercise).

- **Optional: External parties** – If you have little or no experience with organising a cyber crisis exercise, you should consider bringing in external expertise. Use these external experts in strategic planning, to set up exercise resources and to support the exercise leader.

Name	Organisation	Role	Focus	Telephone number
		Project manager		
		Project secretary		
		Communication		
		Project member		
		Project member		
		Exercise leader		

3.1.3. Optional: Programme group

If multiple organisations are taking part in the exercise, it is advisable to set up a programme group in addition to the project team, in which one member from each organisation participates as an exercise planner. For a two-day exercise, allow five days' preparation time for each exercise planner.

For a complex exercise involving multiple participants, it is also advisable to set up a steering group to make strategic decisions. Define the objectives of the exercise together [Appendix 1: Define exercise objectives] and decide on the nature of the exercise [see Appendix 2: Types of exercise]. See also Section 3.1.4 on the steering group.

In conjunction with the programme group, the project group will ensure that the central scenario is defined and implemented. The members of the programme group will also:

- participate in the programme working groups;
- critically review and evaluate the central scenario;
- devise their own institution-specific scenarios;
- draw up the master event list and associated interventions, and supply details for the generic game elements;
- to ensure that the scenario creation process is efficient and that, where necessary, the scenarios fit together, the assistance of the project group and a number of collaborative sessions/workshops may be helpful;

- Based on the information package provided, brief the players in their own team in preparation for the exercise,
- implement the simulation role and give players feedback during the exercise.

Name	Institution	Telephone number

3.1.4. Optional: Steering group

For a complex exercise involving multiple participants, it is advisable to set up an umbrella steering group to make strategic decisions. This steering group consists of members of the participating Gold institutions and will take decisions at the strategic level.

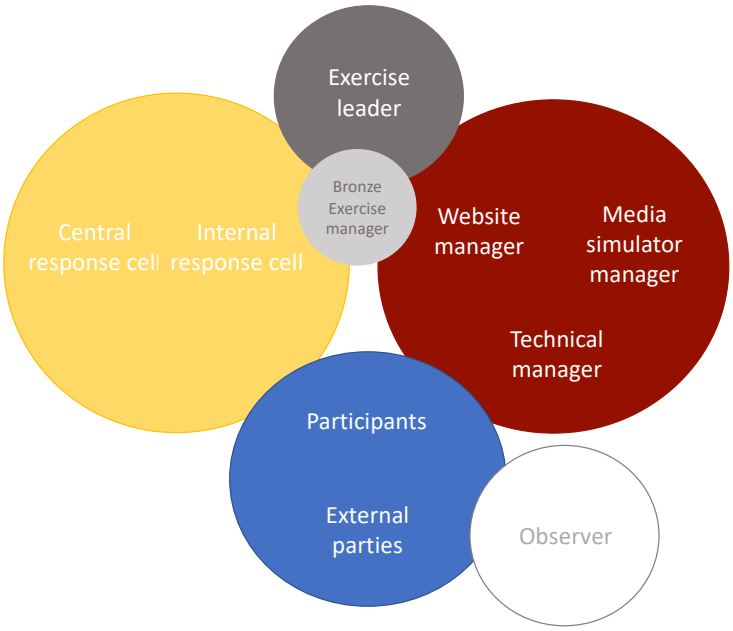
Name	Institution	Telephone number

3.1.5. Participating organisations

- Decide whether the exercise will be internal only or will involve a number of different organisations.
- If the exercise involves multiple organisations, decide, on the basis of criteria such as available preparation time and room capacity, how many organisations can take part.
- Decide at what levels organisations can participate. See [Appendix 3: Roles of participating institutions].

3.2. Roles and tasks during the exercise

During the exercise, the project group, participants and observers each have their own role to play. Below is an overview of the roles that can be deployed in order to ensure that the exercise goes smoothly.



- The **exercise leader** supervises the central scenario, consults regularly with the response cells to find out how the exercise is going within the organisations, and makes adjustments where necessary. This can be done by adding or removing interventions or by offering alternatives to make the exercise as realistic as possible.
- The **central response cell** simulates all the external roles, such as local authorities or other public bodies, emergency services such as the police and fire department, interest groups, journalists et cetera, and rolls out the general game elements.
- The **internal response cell** distributes the interventions throughout the organisation, simulates all the roles of the internal stakeholders who are not participating in the exercise and rolls out the institution-specific game elements.
- **Optional:** An **observer** can be designated for the duration of the exercise. Observers can observe in situ whether, and if so how, the objectives are being achieved. These observations can be used as input for the evaluation process.[4] The observer can also liaise with the internal response cell on the use of interventions to adjust the scenario while the exercise is under way.
- **Optional:** The **media simulator manager** can ensure that the closed system used for media messages is effective and add/correct messages where appropriate.
- **Optional:** The **website manager** manages any websites that are used, and, where necessary, adjusts them in line with the game during the exercise.
- **Optional:** The **technical manager** ensures that any problems that arise during the game can be resolved and that adjustments can be made to malware et cetera.
- **Optional: External parties** are parties that take part in the exercise in their own role; e.g. the General Intelligence and Security Service (AIVD), the National Police Agency (KLPD), the National Cyber Security Centre (NCSC) and the Data Protection Authority (AP).
- **Optional:** A **Bronze exercise manager** who coordinates the contact between infiltrators and institutions on the Capture the Flag exercise, and acts as a source of information regarding the observation of the simulation exercise.

[4] ISO 22398:2013(E), Art. 5.4.2, p. 20

Party	Role
Example: KLPD (National Police Agency)	Example: Involved in the exercise in the context of reporting
Example: NCSC (National Cyber Security Centre)	Example: Participates in the exercise in own role
Example: AP (Data Protection Authority)	Example: Reporting of data breaches 'simulation based on information supplied'

- The **participants** are the players who are confronted with the actions and interventions in their own work environment. They must take actions and make decisions in order to manage the crisis on the basis of the crisis scenario, as if they are actually dealing with a crisis.

For an overview of possible participants and the roles that can be simulated by the response cells during a simulation exercise, see [Appendix 8: Examples of roles of internal players and roles simulated by response cells].

4. Internal information, list of resources and materials

4.1. In preparation for the simulation exercise

- **Central wiki –** For collecting and sharing all minutes, information documents, files et cetera. Where appropriate, make special areas available to participants, project group, programme group and steering group. Also create an **FAQ** (frequently asked questions).

4.1.1. Create scenario

- Use a number of different documents to help you create the scenario. These serve as a basis for the scenario and explain how it should be created.

  Examples of documents include:
  - **questionnaires** designed to define the objectives and scope of the exercise within the institutions;
  - document containing information on **potentially sensitive data** within institutions in order to define the strategic scope;
  - **sample master event list**, to which institution-specific scenario elements can be added;
  - **examples of interventions** such as newspaper articles, blogs, emails, tweets, questions from the Supervisory Board, questions from lawyers et cetera;
  - a **supplementary scenarios handbook** may be supplied to help with creating the scenario;
  - **anonymised example of an institution-specific scenario** – to serve as an example for an institution's own scenario;
  - information for the websites and the **malware and technical elements**;
  - **manual** for delivery and installation of the technical elements.

4.1.2. Information for participants

- **Email to organisation** – explanation of the exercise
- **Sample presentation** – to brief players
- **Email inviting players** to the briefing
- **Information package for players** – comprising:
  - a list of definitions, see [Appendix 17: Definitions];
  - general information about the exercise;
  - rules of play, see [Appendix 11: Rules of play for players];
  - overview of documents to be received, e.g.
    - lead in;
    - teaser;
    - address list.

- **Lead in –** Prior to the exercise (the day before, for example) you can distribute a document that explains the background of the scenario and outlines the current situation in the media and society; that way, all the participants start with the same information.
- **Teasers –** Where appropriate, video clips or other material could be prepared and distributed to players as a warm-up to the game.

4.2. Documents during the exercise

- **Address list –** Create an address list that includes all participants. This guarantees a closed environment, which ensures that the exercise and reality are not confused. Only the participants on this list may be approached. If a person is not on the address list, players should contact the response cell.

- The exercise planners have set out the final version of the institution-specific scenario in a **master event list**, i.e. a combination of events for the generic scenario and institution-specific events.
- The **interventions that have been created**, e.g. newspaper articles, tweets, social media messages, blogs, emails et cetera, as well as the interventions that will be phoned in.

4.3. Communication media during the exercise

In order to ensure that communication is effective, both during the preparation phase and the exercise itself, it is advisable to create separate email addresses, for example for the project group, programme group and steering group.
It is helpful to create an email address that can be used as a central log during the exercise. That way, all communications can be monitored. Participants must include this email address in the “cc field” of every email. It is also advisable to create an email address for contacting the exercise leadership during the exercise, so that participants can approach the exercise leadership directly with any questions or comments they may have.
Not all institutions feature on the SCIRT and SCIPR mailing lists[5]. Consequently, it is advisable to create separate mailing lists for all the institutions taking part in the exercise. That way, no one misses out on relevant information during the exercise.

- Create different **email addresses** for the preparation phase and for the exercise itself:

Target group	Email address
Project group	
Programme group	
Steering group	
Email address for logging of emails	
Email address during exercise for all game-related communications	
Alternative exercise SCIPR address	
Alternative exercise SCIRT address	

- You should also create **internal email addresses** for use during the exercise for:

Purpose	Email address
Email address that is copied to, so you can keep track of all communications	
Email address via which you as a response cell can be contacted	

- Communication media such as **WhatsApp, Jabber et cetera** can also be used. You should also decide which other communication media will be used.

[5] SCIRT and SCIPR are communities of ICT experts from the institutions connected to SURFnet where insights around security are exchanged at operational and policy level.

4.4. Media simulator

Use a closed environment for distributing messages. This ensures that the exercise and reality are not confused. A media simulator can be used for this purpose. Another option is to distribute media messages by email.
A media simulator contains all media messages: e.g. Facebook, Twitter and newspaper reports. Messages can be general or institution specific. In order to prevent unwanted interference in the game, access to the media simulator is restricted to players only. During the game, messages can be added and responses can be made to the social media messages.
Ideally, the media simulator will be pre-programmed and will play the messages automatically during the exercise. Where necessary, the simulator can be used to slow the game down or speed it up. This makes it possible to monitor developments during the game and the pace of the players.

- Decide whether you will use a **simulation environment** and which, or whether you will build the environment yourself.

5. Logistics of the simulation exercise (Gold and Silver levels)

5.1. Duration, dates and location

Duration of exercise – Decide how many days the exercise will last, and decide whether the game will be played during working hours only, including evenings or 24 hours a day.[6]
Dates of exercise – Choose a date or several dates, bearing in mind factors such as holidays and other events.
Location of exercise – The location of the exercise will depend on the type of exercise. In the case of a simulation exercise, the following will apply:

- Players will play at their own location in their own work environment.
- The response cells and exercise leadership will be based at a central location from which they will control the exercise.

5.2. Programme for simulation exercise

Schedule and programme for exercise days

- Prepare the logistical aspects of the exercise days.
- Draw up an overview including the programme for the exercise.
  See [Appendix 14: Example of exercise programme for a cyber crisis exercise].
- Draw up a plan for the exercise days including schedule and resources.
  See [Appendix 15: Example of plan for exercise days].

You should also think about catering and the time required for transportation, e.g. to get game leaders to a central location.

Procedure in a simulation exercise

- In a simulation exercise, players practise in their own environment and the exercise is controlled from a central location by the response cells. For an example of the procedure involved in a simulation exercise, see [Appendix 9: Procedure involved in a simulation exercise].

5.3. Briefing of participants, organisation and response cell

- Before the exercise starts, **brief participants** on the exercise. Discuss the objectives of the exercise, the rules of play and mutual expectations.
- Decide whether you will notify the organisation about the exercise in advance and how much detail you want to provide.
- Briefly discuss the objectives of the exercise, the expectations and the details of the exercise with the response cell before the exercise begins. For more details, see [Appendix 12: Briefing of participants, organisation and response cell].

[6] OZON was played during working hours only for logistical reasons, and because it was the first time an exercise like this took place.

6. Optional: Observation and Capture the Flag exercise (Bronze)

6.1. In preparation for the Bronze exercise

During the OZON exercise, Bronze participants were able to monitor how the exercise developed for gold and silver participants, as well as participate in a ‘Capture the Flag’ exercise.

Observation
Participants receive login details a few days in advance so they can follow the crisis during the simulation exercise via the media simulation environment. If media messages are distributed by email, these messages can also be sent to the Bronze participants.

Capture the Flag
It may be decided that in addition to the observation of the crisis exercise, a game element is to be added. During the OZON exercise, managing multiple exercise systems simultaneously proved difficult. This element can also be played separately.

Tasks;
- Arrange for students or volunteers to act as infiltrators for the Capture the Flag task.
- Create 'attack software' that must be detected by the institutions.
- Instruct the infiltrators on the use of a laptop and use of the malware.
- Make sure that no actual damage is caused, do not add additional functionality to the malware that is superfluous to the exercise, and instruct the infiltrators to abide by the rules.
- Plan a test session with the infiltrators to make sure everything is working properly.
- Provide infiltrators with proof of exemption to formalise that the institution, or institutions, requests their presence and allows for the use of the software on the infiltrators’ laptops.
- Liaise with an exercise planner at the institution who can manage the exercise internally.

6.2. Programme for Bronze exercise

Observation
- Participants can log into the media simulation environment and follow the messages during the day. If media messages are distributed by email, they will receive the same messages as the Gold and Silver players, but do not need to act on them.

Capture the Flag
- Infiltrators enter the premises of the Bronze institution early in the morning and keep moving around in the building(s) of the institutions. As a result, they are not detected immediately. As the day progresses, they can stay in one place so they are easier to find. They carry a laptop containing simulation malware.
- Interventions can be made in order to get the institutions on the right track.
- At the end of the day/exercise, participants are told about the threat that was present, and, if they have not yet detected the threat, are told how they could have done so. The logfiles are also released to enable further investigation.

7. Evaluation

Structured monitoring and evaluation help apply the feedback and lessons learned across the organisation. When evaluating the exercise, you should draw on the experiences of participants, the preparation team and the observers. Reflect on these experiences together in evaluation sessions. You can also use an online survey to obtain the views of the project group, the programme group and the participants.

7.1.1. Evaluation points

Schedule a number of different evaluation points:

- **Hot wash/during the game –** During the game, players can be given a checklist/questionnaire to monitor their experiences immediately. This can be used to inform subsequent evaluation sessions, so the key evaluation points remain top-of-mind. Players can mention both issues relating to the exercise itself and issues relating to the internal processes. The exercise can also be jointly evaluated by sub-groups during the exercise itself or at the end of the first day and interim results can be discussed.
- **Immediately after the game –** Organise an evaluation session in the afternoon immediately after the game. If only one institution is involved in the exercise, you can discuss conclusions from both the exercise itself and the internal processes. If multiple organisations are involved, it is a good idea to decide whether you will evaluate the exercise only or the organisations' internal processes as well. Since content-related processes can be sensitive, consider to evaluate these internally only, rather than in a group.
- **A few weeks after the game** – Discuss with the exercise leadership (project group, programme group and steering group) how the exercise went and its results.
- **A few weeks after the game –** Find out what all the teams in the player's internal organisation thought about the exercise and describe general conclusions and experiences.

7.1.2. Levels

The results of the exercise can be evaluated at different levels.

- **Exercise process** – Establish whether or not the exercise was successful. The focus here is on the organisation of the exercise and how the exercise was perceived by the preparatory team and the participants.
- **Internal crisis management structure –** Evaluate how the organisation's crisis management structure worked during the exercise. This can be done across the board, including all participants/institutions and/or within the institution itself.
- **Sharing of knowledge between organisations –** If multiple institutions took part in the exercise: evaluate whether/how the players collaborated with and shared knowledge with each other.

7.1.3. Internal observer

- The observer can observe in situ whether and how the objectives are being achieved. These observations inform the evaluation process. The observer also liaises with the internal response cell on the use of interventions to adjust the scenario while the exercise is under way.

7.2. Dates, location, format

- Plan at what point you wish to evaluate the exercise.
- Plan what you want to evaluate.
- Choose the format of the evaluation (e.g. a meeting, a survey, by team, with a complete group of participants).
- Choose the location of the evaluation and decide who will be invited to take part.

7.3. Survey

As soon as the exercise is over, online questionnaires containing questions about the exercise process and/or questions about the achievement of the (internal) exercise objectives, own experiences, successful aspects of and learning points from the exercise can be sent to participants.

- Devise questions for the survey
- Launch the survey after the exercise
- Incorporate the results of the survey into the overall evaluation

For background information, see [Appendix 16: Evaluation.]

Appendix 1: Define exercise objectives

Primary and secondary objectives

The main objective of the OZON Cyber Crisis Exercise was:
- to increase the resilience and awareness of institutions in the event of a cyber crisis.

The secondary objectives were:
- to test the functioning of the internal and external chain;
- to test the effectiveness of crisis communications;
- to improve cooperation within and between institutions.

Internal exercise objectives

Institutions defined internal objectives based on the primary and secondary objectives of the exercise.

The most common internal objectives were:
- to raise awareness of security;
- to raise awareness of cyber risks;
- to test internal and external communications;
- to test prompt evaluation;
- to improve communications between operational and management levels;
- to test whether internal processes can handle a cyber crisis effectively;
- to test security protocols.

Other objectives could be:
- to test collaboration with external partners;
- to test collaboration within the information chain.

Appendix 2: Types of exercise

This plan describes a major cyber crisis communication exercise. There are various types of exercises with varying degrees of intensity and scope. An overview of the various types of exercise can be found below.

Crisis exercises can be divided into two types:

1. **Discussion-based exercises**[7] to familiarise participants with plans, policies and procedures. In discussion-based exercises, a dilemma is presented to participants and they discuss the dilemma within predefined parameters.

2. **Practical exercises** are used to test plans, policies and procedures and to train employees. Generally speaking, the simulation environment reflects a realistic environment.

Examples of discussion-based exercises

- **Desk Check –** A desk check is a method used to validate plans and procedures and any changes to them. It is usually done in discussion with the author of the plans and procedures. The plans and procedures are reviewed step by step on the basis of a scenario. This makes it clear what steps are needed and how they should be executed.

- **Walkthrough** – A walkthrough takes a closer look at a specific scenario, such as a cyber crisis. A walkthrough demonstrates who does what and when, and what actions can be taken. In a walkthrough, the various steps in a crisis, from detection to escalation, response, follow-up and closure, can be reviewed in a very specific way. On average, a walkthrough takes half a day. A walkthrough can be implemented internally or with other partners who play a role in the crisis.

- **Workshop** – In a workshop, as well as working through a scenario step by step, participants can also discuss the various responses and actions. The responses and actions of teams and individual participants can be rehearsed without time pressure. This will help people deal effectively with crisis situations and scenarios.

- **Tabletop exercise** – A tabletop exercise covers aspects of crisis management. Players receive the same information in advance about the simulated crisis situation and their role. During the exercise, players can use simulated (media) messages. The crisis team can share relevant information with the tabletop, obtain an overview and take (appropriate) decisions and (communication) measures.[8] A tabletop exercise is a good option if you want to test out the crisis management structure and practise collaboration in a relatively calm environment and/or train people in specific skills. A tabletop exercise is also a good option if an organisation is not (yet) ready for an interactive simulation exercise.

Examples of practical exercises

- **Comms check** – A comms check is used to check and validate communication methods and notification systems.
  This type of exercise is used to check the systems and infrastructure and to test whether everything is working effectively.

---

7 ISO 22398:2013 also calls them "dilemma exercises"; Art. 5.2.13, p. 16
8 http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ (consulted on 5 September 2016)

- **Response exercise** – This is used to test whether you can convene a crisis team within the agreed period.

- **Distributed tabletop exercise** – In a distributed tabletop exercise, plans and procedures are worked through on the basis of a scenario, with players playing their usual role.
  The set-up is similar to a tabletop exercise, but there is no opportunity for discussion. Participants must act as though a crisis is actually taking place. Possible responses can be discussed subsequently in an evaluation, where appropriate. The advantage here is that participants can practise their actions in their routine environment.

- **Command Post Exercise (CPX) –** In a CPX (sandbox exercise), a crisis is simulated without the use of emergency services, external environmental factors or players. The crisis teams tackle questions and tasks in a realistic and evolving scenario. The teams can practise their actions and responses to a changing scenario in their own environment, with their own facilities.

- **Simulation exercise** – In a simulation exercise, participants enact a realistic scenario in their own environment. Participants practise as much as possible under normal circumstances, with their own resources in their own environment. The scenario develops as a result of their decisions and actions. A simulation exercise is appropriate if the aim of the exercise is to practise under pressure and to test and train the responses of participants in their own environment. The intensity of the exercise and how the scenario develops will depend on the number of participants and their level of experience. It is also important to decide whether only internal parties will participate or whether external parties will be involved as well. A simulation exercise can take anything from half a day to several days.

- **Capture the Flag** – In an operational Capture the Flag exercise, the aim is to find a 'flag' or other item and 'capture' it. This can be done in teams or individually, and in competition with others or otherwise. In a cyber-related Capture the Flag exercise, the aim is often to detect and catch hackers who target (simulated) ICT systems.

- **Red Team/Blue Team** – In a Red Team/Blue Team exercise, the red team attacks the network or another important business service and the blue team tries to foil the attack. This exercise increases awareness of potential risks. The exercise also provides an insight into potential vulnerabilities and ways of tackling them, as well as insights into strategies for detecting and responding to an attack.

User-friendly examples of exercises can be found in Linux Journal.[9]

[9] https://www.linuxjournal.com/content/example-security-exercises (consulted on 21 December 2016)

Appendix 3: Roles of participating institutions

These requirements were set for OZON. Decide for each exercise if you wish to maintain these requirements or set new ones.

Level	Content
Gold	The institution provides at least five participants. At this level, players are employees who take strategic decisions, such as members of the Executive Board.
Silver	The institution provides a minimum of three people from the organisation. It is not necessary for these individuals to be part of the strategic crisis team as the exercise is conducted primarily at operational level.
Bronze	Institutions primarily act as observers. They monitor the progress of the exercise and follow the proceedings. You may choose to add a Capture the Flag exercise or something similar.

Appendix 4: Prerequisites for the success of the exercise

- **The duration of the exercise** will depend on the exercise objectives, the availability of participants and the impact on the organisation (holidays et cetera). An exercise can take anything from a few hours to a few days. Some types of exercise can take several weeks. In that case it will not be a full-time exercise, but will comprise tasks alongside existing activities.

- **Impact on operational processes:** You may choose not to disrupt day-to-day operations too much and to keep the **impact on operational processes** within the organisation to a minimum.

- **Impact on infrastructure:** To avoid impact on the existing infrastructure, a simulation environment that simulates the existing production environment can be used. You can build this environment yourself or have it built for you. For technical impact, you can, for example, also use simulation malware and Raspberry Pi's. The institutions themselves can decide whether or not to use these.

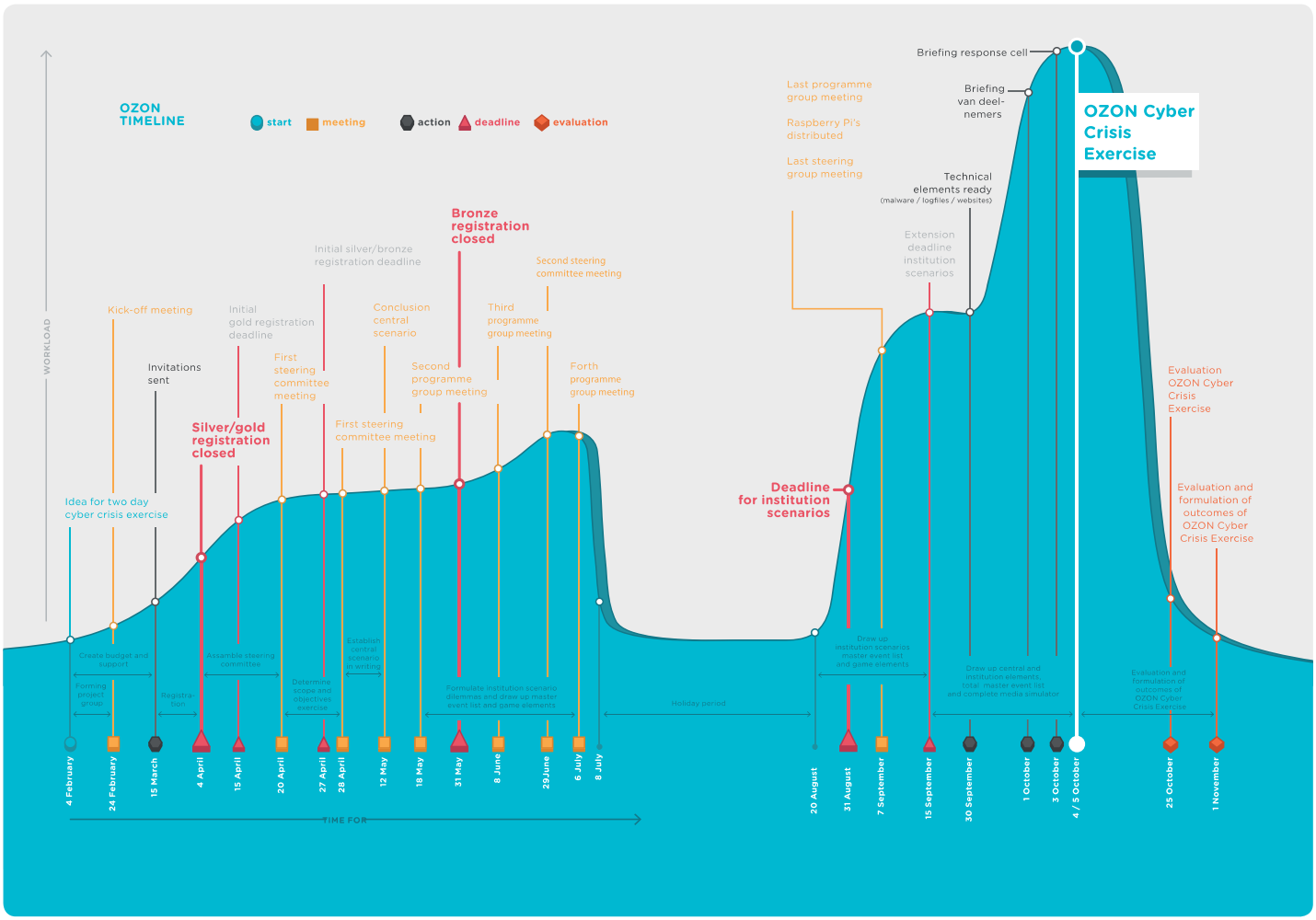
- **Role of security officers:** When security officers are members of the preparation team as exercise planners, they do not take part in the exercise in their own locations. In the case of OZON, institutions found suitable solutions to this problem themselves. This gives institutions an opportunity to see how the organisation functions in the absence of the security officer.

- **Exercise planners:** When designing the scenario, specific knowledge of the organisation is required. Therefore, you should establish in advance who has this knowledge, who will prepare the exercise as an exercise planner and who within the institution will devise the potential institution-specific scenario. Keep in mind that exercise planners cannot take part in the exercise itself.
-
- **No-play situation:** During the course of the exercise, unforeseen circumstances may arise that prevent play from continuing. In this event, the exercise will be suspended. The authority to stop the exercise (No Play situation) lies with the project manager.

- **Guarantee closed environment:** To avoid an exercise scenario being perceived as an actual crisis, measures must be taken to guarantee a **closed environment**. The exercise leadership will draw up rules of play to ensure this. A 'closed' address list of participants and a closed environment for distributing messages ensures there is no mixing up the exercise and reality. Only the participants on this list may be approached. If a person is not on the address list, the response cell should be contacted.

Appendix 5: Planning timeline for OZON 2016

The figure below shows a visual representation of the timeline, including dates, deadlines and actions for the organisation, execution and evaluation of a cyber crisis exercise. This timeline represents the schedule and organisation that was used in the OZON 2016 Cyber Crisis Exercise. You can find a detailed timeline/plan containing tasks/dates and responsibilities in [Appendix 6: Timeline for organisation of OZON Cyber Crisis Exercise].



Appendix 6: Timeline for organisation of OZON Cyber Crisis Exercise

The timeline below is an example of the schedule that was used for the OZON Cyber Crisis Exercise. The various activities are described in detail in the guidance and appendices.

Category	Date	Activity	Responsibility
START	**4/5 February**	**Start of organisation of cyber crisis exercise**	
Activity	Between 4/5 February and 24 February	Establish client; Set up project group.	
Activity	Between 4/5 February and 24 February	Define main objective of exercise; Define type of exercise; Define duration, dates and locations of exercise.	
Activity	Between 4/5 February and 15 March	Create budget and generate support.	
Activity	Between 24 February and 15 March	Book locations and plan and document facilities for the exercise, such as lunch. For details, see also the plan for exercise days appendix.	
Meeting	24 February	Kickoff meeting	
Activity	24 February	Decide on name for exercise.	
Activity	24 February	Central wiki in progress.	
Activity	15 March	Send invites to participants.	
Activity	Between 15 March and 27 April	Participant registration period.	
Deadline	**4 April**	**Gold/Silver registrations for OZON closed early due to the large number of applications.**	
Activity	Between 4 April and 20 April	Form steering group from Gold members.	
Meeting	20 April	First meeting of steering group.	
	20 April	Draw up need/nice to have list with steering group.	
Activity	20 April	Define exercise criteria.	
Deadline	**27 April**	**Official deadline for Gold/Silver applications**	
Meeting	28 April	First meeting of programme group	
	28 April	Decide on dates and content of evaluations.	
Activity	28 April	Define scope/exercise objectives of participating institutions. Draw up need/nice to have list.	

Activity	Between 28 April and 12 May	Write central scenario.	
Activity	Between 28 April and 18 May	If you are using a media simulator, decide which and/or whether you will build it yourself.	
Activity	Between 28 April and 18 May/refinement by 15 September	Devise communication strategy and plan.	
Meeting	12 May	Finalisation of central scenario.	
Meeting	18 May	Second meeting of programme group.	
Activity	Between 12 May and 8 July	Draw up overall schedule for exercise days. See [Appendix 15: Example of plan for exercise days].	
Activity	Between 12 May and 5 September	Send invitations to external partners, e.g. police, NCSC et cetera	
Activity	Between 12 May and 15 September	Produce and discuss documentation - Lead in - Information package for players - Email to organisations - Player briefing materials - Email inviting players to briefing - Address list - Teasers (where appropriate)	
Activity	Between 12 May and 15 September	Generate support among the players within the institutions.	
Activity	Between 12 May and 15 September	Decide whether you will use an observer for internal observation and, if so, organise observers.	
Activity	Between 18 May and 8 July	Formulate dilemmas for institution-specific scenarios and draw up master event list, develop game elements and technical elements.	
Deadline	**31 May**	**Bronze registrations closed**	
Meeting	8 June	Third meeting of programme group.	
Meeting	29 June	Second meeting of steering group.	
Meeting	6 July	Fourth meeting of programme group.	
Holiday	8 July to 20 August	Holiday period	
Activity	Between 20 August and 31 September	Create institution-specific scenarios master event list, game elements and technical elements	
Deadline	**31 August**	**Deadline for institution-specific scenarios**	

Activity	Between 1 September and 15 September	Review level and content of institution-specific scenarios.	
Meeting	7 September	Final meeting of programme group	
Activity	7 September	Distribute Raspberry Pi's.	
Meeting	7 September	Final meeting of steering group	
Expiry of deadline	**15 September**	**Expiry of deadline for institution-specific scenarios**	
Deadline	15 September	Documentation complete.	
Activity	15 September	Communication media for the exercise itself – in progress.	
Activity	Between 15 September and 4 October	Develop central and institution-specific elements. (Both technical and strategic.) Create overall master event list. Fill media simulator with interventions.	
Activity	Between 15 September and 4 October	Send email to participants inviting them to briefing.	
Activity	Between 15 September and 4 October	Brief players and organisation.	
Activity	Between 15 September and 4 October	Send email to organisation about exercise.	
Activity	30 September	Technical elements ready (malware/log-files/websites/simulation environment/attack software for the Bronze exercise)	
Activity	30 September	Brief infiltrators on Bronze exercise and send proof of exemption to infiltrators.	
Activity	30 September	Briefing of participants	
Activity	3 October	Briefing of response cell	
EXERCISE	**4/5 October**	**OZON Cyber Crisis Exercise**	
Evaluation	5 October	Hot wash evaluation of OZON Cyber Crisis Exercise	
Evaluation	**25 October**	**Evaluation of OZON Cyber Crisis Exercise** with project, programme and steering group	
Activity	Between 5 October and 1 November	Evaluation and formulation of outcomes of OZON Cyber Crisis Exercise.	

For a checklist based on the above deadlines, see [Appendix 18: Checklist for organising a (cyber) crisis exercise based on the OZON model].

Appendix 7: Creating a scenario for a simulation exercise

Central scenario
On the basis of predefined exercise objectives, you will design a scenario that offers the institutions sufficient points of reference. See [Appendix 1: Define exercise objectives]. Each department and/or institution can link its own scenario to this central scenario. Design the scenario in such a way that it acts as a starting point for the institution-specific scenarios of both the Gold and Silver players. These scenarios form the basis of the cyber crisis exercise.

Create a situation that requires players to scale up and escalate, in order to make the scenario attractive to the Gold players, who include, among others, members of the Executive Board. Bear in mind the availability of the Executive Board and establish whether they will join for a specific period of time or whether they will play the whole time.
Make sure the scenario allows the impact to be greater on some departments/institutions than on others. That way, the scenario can be adapted as required.

Basic principles of scenario
Before you write the scenario, draw up a **need/nice to have list** with the programme group/steering group, which creates the criteria for the scenario.

Example criteria for the scenario include:
- the participants can practise both internal communication and escalation to strategic level;
- the exercise must provide sufficient challenge for both crisis management and IT departments;
- the scenario must contain sufficient recognisable and realistic elements for all the different institutions taking part in the exercise;
- the scenario must include enough complex dilemmas to determine whether participants can make decisions in time;
- to ensure that the crisis cannot be resolved without involving the strategic level, both technical and strategic dilemmas that participants cannot solve without taking a strategic decision can be included;
- to ensure that institutions have to coordinate with each other, the game could include an ethical element.

Examples of dilemmas that require the attention of the Executive Board include:
- damage to image;
- claims;
- personal reputation;
- reputation of the organisation;
- directors' liability;
- ethical issues.

These dilemmas could involve the following risks:

- disclosure of:
  - medical records;
  - personal data;
  - research data;
  - business data;
  - organisation data;
- extortion;
- encrypted data files;
- espionage;

- modified/manipulated data.

Central Scenario (Example scenario)
The central scenario of OZON consisted of two simultaneous threats: an attack by an idealistic hacker group and a criminal component.

Based on the above-mentioned principles, in the case of OZON, part of the exercise involved a fictitious idealistic hacker group that many Dutch people (including those within the institutions) had sympathy for. This group had both an ethical and a criminal component, so that simply ignoring the dilemmas wasn't an option. The threat posed by these hackers affected the entire education and research sector. This encourages cooperation between the institutions.

The hacker group believes that companies and authorities are in possession of too much information and that this information is not being made public for economic reasons. Their view is that if all data were available to everyone, the development of human civilisation would be accelerated. Failure to share information hinders progress, which is why they strongly disagree with all forms of intellectual property. Their goal is to make as much data as possible fully available to the public. They do not take the sensitivity of personal data into account.

The hacker group is popular with the public as a result of its revelations, and has now announced that it is expanding its activities to include the Netherlands, where one of its targets will be the education and research sector. For the hackers to achieve their goal, the scenario has a strong technical component. They have distributed malware on a large scale. This is multifunctional malware that can not only collect and transmit files, but that can also encrypt all the files on-demand on a computer or connected network. This has allowed the hacker group to collect large quantities of sensitive data. The hacker group will make this data public in a media offensive.

Employees of Dutch education and research institutions are prompted by the group to download the malware executable and install it on their institution computers. The executable propagates itself via a Windows zero-day vulnerability, thereby enabling additional data to be collected. A request is also made to create a mirror of the website containing disclosed data. Raspberry Pi units are used to run these mirrors.

Initially, a number of professors expressed their support for disclosure of the data. Although they condemn hacking, they are in favour of the revelations because they are related to ethically unacceptable research. An online petition that researchers can sign is also launched.

The scenario also has a criminal component. A journalist discovers a web portal where grades can be adjusted for a fee, grades can be published, medical records of famous Dutch people can be published, compromising photos of students and lecturers can be displayed and exam data can be consulted. A possible link to the hacker group is suggested, but it is not clear whether it is genuine.

Institution-specific scenarios
The central scenario has an impact on the entire education and research sector and creates a cyber crisis that affects all institutions across the board. Where multiple institutions are taking part in the exercise, institutions may be allowed to write their own institution-specific scenario based on the central scenario. This modular approach allows each institution to adapt the exercise to its own requirements. This scenario will be based on the institution's own exercise objectives: see [Appendix 1: Define exercise objectives], participants and exercise situation. In this context, specific attention can be paid to what information is sensitive and which systems may contain this information.

For example, one institution may be adversely affected by the disclosure of research on animal testing or controversial research into the effects of sugar on children; others may, for example, be adversely affected by the disclosure of files containing details of students' mental health. In the case of hospitals, patient data and drugs usage data may, for example, be disclosed.

In addition, directors' expenses claims could be exposed. This represents a huge threat to the image and reputation of the organisation and to personal reputations, and can even result in directors being held liable or in claims for financial compensation. These difficult technical and strategic dilemmas, which cannot be resolved without a Board-level decision, allow participants to practise both internal communication and escalation to the highest level of management.

Regarding the criminal component, it could be possible to manipulate for example grades, examination data, degree data and even medication data after paying a fee. To create confusion and encourage collaboration, it stays unclear whether the same hacker group is responsible for this.

Appendix 8: Examples of roles of internal players and roles simulated by response cells

Players can be:	**Simulated by internal response cell:**	**Simulated by central response cell:**	**External partners involved in the exercise, e.g.**
- Departmental managers - Lawyers - Communication officers - Press officers - Incident Response team - Security Officers - Privacy Officers - Members of the Executive Board - Staff departments - Board members - ICT managers - Service desk staff - Faculty staff	- Non-participating employees - External partners - Stakeholders - Students - Patients - Lecturers - Professors	- Journalists from newspapers such as: - NRC - Trouw - Nu.nl - AD - Faculty newspapers - Data Protection Authority - Mayors - Members of the Supervisory Board	- National police - NCSC (National Cyber Security Centre)

Any role that is not actually involved in the exercise can be simulated.

Appendix 9: Procedure involved in a simulation exercise

In a simulation exercise, participants play out a realistic scenario in their own environment. Participants practise as far as possible under normal circumstances, with their own resources in their own environment. The scenario develops as a result of their decisions and actions.

Distribution of the first interventions sets the scenario in motion and triggers the first actions. The response cells then provide interventions to keep the exercise going. The participants respond accordingly. This generates interaction between the participants and the scenario. The pressure on the participants grows as the exercise develops. This prompts many actions and decisions and a great deal of communication.

Interventions may require both technical and strategic actions and decisions. An intervention that displays a login error, for example, may lead to an investigation of the (simulated) production environment. A newspaper report that discloses sensitive information will lead to a response from the Executive Board. Scenarios in which participants are not able to apply a technical measure without a strategic decision are of particular interest. In this case, the technical as well as the strategic level will have to communicate actively with each other.

At the end of the exercise, it will be scaled down and terminated through a 'freeze', a message to all players to stop the game. Unexpected situations may occur during an exercise, e.g. if a participant thinks an actual crisis is unfolding or if an actual emergency occurs. In such situations, the exercise leader and response cells must be flexible and able to improvise. The exercise leader can suspend the exercise or stop it completely.

Appendix 10: Development of technical elements

In order to make the exercise as realistic as possible and to give the engineers enough to do, a number of different technical components can be created and implemented within the exercise.

In the case of OZON for example, a website for the hacker group was built with a foreign cloud provider and updated during the course of the exercise. This website displayed data sets that had been stolen from the participating institutions. The website was mirrored on various locations, including Raspberry Pi's that had been concealed at ten or so institutions. Some participants had made copies of production environments for their own scenario in which the engineers had to look for clues as they would do in real life. Logfiles of hacking activities could be found on the 'contaminated' PCs. The exercise planners distributed these within their own institutions. These logfiles were used to analyse what had happened. The logfiles were downloaded from the command-and-control server.

Finally, for the OZON exercise, malware that communicated with a command-and-control server (which downloaded logfiles of what the malware had allegedly done) was also developed. This was used, among others, for the Capture the Flag exercise for the Bronze participants. To distribute this malware, infiltrators with a 'contaminated' laptop were used, who visited the participating Bronze institutions.

One of the key components of the exercise was to simulate media messages. Using an interactive simulator, newspaper reports were disseminated and Twitter and Facebook were simulated, and the players could react to them. Just as in real life, the media simulator bombarded the players with a wealth of information and misinformation, which increased the pressure on the teams. Keeping track of all the media messages was a job in itself, and made dividing tasks within a crisis team a challenge.

The technical preparation team prepares the technical elements. Institutions supply any information that is required to configure/create the technical elements and generate leads. A decision must be taken as to which leads should and should not be included in the technology. In the case of OZON, it was decided to include all leads starting September 1st. (OZON was carried out on 4 and 5 October 2016).

Examples of technical elements include:
- websites;
- malware;
- Raspberry Pi's for distribution purposes; these could, for example, mirror sites of the websites;
- VMware;
- simulation environments that simulate existing production environments;
- media simulator.

Appendix 11: Rules of play for players

Rules of play

The rules of play include the rules governing the game and the players.

The rules of play must include:

- email address for communication during the game;
- the term that must be used in any form of communication;
- how to contact people you need during the game;
- employees who are taking part in the game will be included in an address book;
- employees who are not taking part in the game will be simulated by the internal response cell;
- the start of the game;
- ending the game;
- the contact for all internal queries (the project manager);
- the central contact for all queries (exercise leader for central game);
- suspension of the game in the event of interruptions;
- stopping of the game in the event of unforeseen circumstances – NO PLAY rules;
- rules for excluding participants;
- rules for what material constitutes evidence and, in particular, from when.

Expectations of players

- The aim is that players will respond as they would do during a normal working day.

Appendix 12: Briefing of participants, organisation and response cell

Briefing of participants
Brief participants on the exercise before the exercise starts. This can be done through a meeting where you explain to the players:
- the objective;
- the rules of play;
- the mutual expectations.

This will help ensure that the exercise goes smoothly.

In this context, you can use a presentation and invitation and:
- information package;
- rules of play;
- address list;
- background information;
- lead in;
- teasers.

Briefing of organisation
It may be that non-players within the organisation come into contact with the exercise. You can tell them about the exercise in advance so they are not under the illusion that an actual crisis is taking place. In order to avoid unintentional 'participation' by third parties, don't provide too many details about the content of the exercise.

Briefing of response cell
You can hold a short start-up briefing with the response cells prior to the exercise. Discuss the objectives of the exercise and agree on the use of premises, telephones and address book. You can also discuss the rules for the role-play and briefly run through the scenario again. You should also discuss the rules for interrupting the exercise, where appropriate.

Appendix 13: Content of a communication plan

Think about the communication target groups, objectives and events.

Target groups
- **Government**
  Ask questions such as:
    - Do you need to communicate with the government?
    - And will you simply notify them or will your message have other content too?
- **Internal/Institutions**
    - Who within your organisation/the organisation(s) do you want to reach through the exercise? (directors, security officers, ICT staff, ICT directors?)

Before the crisis exercise
- **Internal and external communication** – Will you tell people that an exercise will take place and specify the content of the exercise? In the case of OZON, caution was exercised with regard to the press in order to avoid 'unwanted players'. Internally, non-participants were told just before the exercise started that an exercise was about to take place but the exact date was not specified.
- **Invite participants** – Make sure you invite people to take part in the exercise in good time so they have time to consider whether they want to be involved. For this purpose create communication means to inform people of the options, the objectives of the exercise and details such as time, location and facilities.
- **Invite internal players** – Invite players to participate in the exercise in their own roles. Produce invitations and briefing materials to explain to them the objectives of the exercise, the benefits of taking part and, just before the exercise begins, the rules of play et cetera.

During the exercise
- **Video** – Will the exercise be filmed? (Make a separate plan for this.) SURFnet made a video of the crisis exercise with an overarching story. This explained what the crisis exercise was, indicated how many institutions took part in it and what participants learned from it, and gave a sense of the atmosphere during the exercise.
- **Press releases** – Will you tell people immediately after the exercise that a crisis exercise has taken place? In the case of OZON, it was decided to issue a press release that stated that a crisis exercise had taken place within the education and research sector, specifying the number of institutions that took part and drawing a number of overarching conclusions. The press release was sent to the institutions in advance. SURFnet sent the press release to a number of different media.
- **Articles** – Are there journals in which you want to put an article? Who would you allow to write such an article? This could perhaps be an interview with a security officer, a student or an ICT-employee who talks about their part in the exercise and what they will do with the results.

After the crisis exercise
- Will you communicate the **results, outcomes and lessons learned from the exercise** internally and/or externally? In the case of OZON, a decision was taken to share general learning points broadly but to keep the institutions' internal learning points internal.
- Are there **conferences and meetings**/other events at which you would like to present/share the outcomes of the exercise?
- Will you communicate the **results and areas for improvement from the evaluations** internally for the internal crisis organisation and, if so, how?

Appendix 14: Example of exercise programme for a cyber crisis exercise

Day	Time	Part of exercise
Tuesday 4 October 2016	8.15am-7pm	Decentralised part of exercise: Day 1
Wednesday 5 October 2016	9am-12 noon	Decentralised part of exercise: Day 2
Wednesday 5 October 2016	2pm-5pm	Centralised part of exercise: evaluation
Wednesday 5 October 2016	5pm-7pm	Social event

1.1.1.1 Exercise programme – Day 1

Day 1: Tuesday 4 October			
Phase and participants		**Overall timeline**	**Programme components and scenario developments**
Introductory phase	**Emphasis: technical/operational level**	8.15am	Start of exercise at own location
			Technical Interventions scenario
			Hackers specify in the media what their objective is and that organisations have been hacked. The nature of the organisations is specified but specific organisations are not yet named. The information is later published online.
			Employees of organisations state in the media that they sympathise with the hackers.
			Information from various organisations is online. Media get involved. Initial consequences for the organisation are clear
Acute phase	**Strategic level involved (this may be within a restricted timeframe e.g. 1pm-3.30pm)**	12.30pm	Journalist asks questions about (technical part of) scenario over the phone.
		1pm	The impact of the scenario is clear in organisations. This is partly because critical articles are appearing in the media but also because employees and clients (students/patients et cetera) are getting worried. Internal and external concern.
		1.30pm	Article about scenario goes online, specific organisations are named. The article is a trending topic. Organisations that have not been named may still be approached with questions over whether they can guarantee that their systems have not been hacked and manipulated too (social media rumours).
		2pm	Staff are involved in spreading data further (this depends on the choice of the organisation, contamination by website visit or actively downloading), possibly because documents are emailed to an email address that belongs to the hackers
			Regulators ask questions about the hackers, on the one hand about the preparedness of the organisation and, on the other, about situation and measures.
		2.30pm	Speculation around follow-up actions and follow-up documents that may be disclosed. Hackers announce follow-up plans on website.

		2.30pm-4.30pm	Critical questions are asked about specific documents and 'irregularities' within the organisation. Blackbooks for each organisation can be found online. The public is asked to help by supplying information. An appeal is made to staff to help clean up the organisations. Some staff don't send information externally, but send it directly to strategic level in order to obtain an opinion on what in their view are irregularities.
		5pm	End of Day 1

1.1.1.2 Exercise programme – Day 2

Day 2: Wednesday 5 October			
Phase and participants		**Overall timeline**	**Development**
Rounding off and reporting	**Technical/operational**	9am	Start of second day of exercise at own location
			Follow-up scenario input. 12 noon – end of exercise.
Travel time		12 noon-2pm	Travel from own organisation to central meeting in Utrecht
Reflection and evaluation		2pm	Reflection on scenario. Mixed teams with a similar background (e.g. technical, policy) reflect on the scenario on the basis of a number of specific questions.
		3.15pm	Break
		3.30pm	Learn lessons and improve and discuss own actions in teams.
		5pm	Document final responses from plenary session
		5.30pm	Closure and social event

Appendix 15: Example of plan for exercise days

Day 1: Tuesday 4 October 2016			
Time	**Action**	**Who**	**Where**
7am	*Prepare for arrival of exercise planners and prepare game* • *Check materials* • *Connect laptop to screens* • *Connect telephones* • *Prepare tea/coffee* • *Set up rooms* • *Someone from automation on hand for support*	*Project secretary and project group*	
7.30am	Welcome exercise planners • Distribute necessary materials • Agree roles and tasks • Launch media simulator	Exercise planners and project group	
8am	Prepare start of exercise • Everyone takes up position	Exercise planners and project group	
8.15am	START OF GAME (see Game overview/Master event list)		
12 noon	(Where appropriate) Prepare lunch for exercise planners and project group	Project secretary	
12.30 pm	Lunch (where appropriate during the game)		
5pm	END OF GAME		
5pm	Brief internal evaluation		
5.30pm	END		
	In the interim: Top up tea/coffee		

Day 2: Wednesday 5 October 2016			
Time	**Action**	**Who**	**Where**
7.45am	*Prepare for arrival of exercise planners and prepare game* • *Check materials* • *Connect laptop to screens* • *Connect telephones* • *Prepare tea/coffee* • *Set up rooms*	*Project group*	
8.15am	Welcome exercise planners • Distribute necessary materials • Agree roles and tasks • Launch media simulator	Exercise planners and project group	
8.45am	Prepare start of exercise • Everyone takes up position	Exercise planners and project group	
9am	START OF GAME (see Game overview/Master event list)		
12 noon	END OF GAME		

12 noon	Prepare lunch for exercise planners and project group (or arrange for it to be prepared)		
12.30 pm	Serve lunch		
1pm	Get rooms ready for evaluation • *Check materials* • *Rearrange rooms*		
1.30pm	Start welcoming players @SURFnet		
2pm	START OF EVALUATION		
5pm	END OF EVALUATION		
5pm	Set up social event (or arrange for this to be done)		
5pm	Social event		
7pm	END		
7pm	Start clearing rooms	Project group	
8pm	Where appropriate, additional session with project group (with food?)		
	In the interim: Top up tea/coffee		

Appendix 16: Evaluation

Evaluation of the exercise
The outcomes of the exercise can be evaluated at various levels. First, you can establish if the exercise was successful. In this case, the focus is on the organisation of the exercise and how it was perceived by the preparation team and the participants.

Possible questions include:
- How did the preparation phase go?
- What did people think about the intensity of the exercise?
- Was the scenario successful, and was the number of interventions adequate or not enough?
- Did the scenario have the desired impact?
- Did the participants find the scenario realistic?
- Were there situations that had an impact on the execution of the exercise?
- Are there any recommendations for future exercises?

Evaluation of internal crisis processes
In addition to evaluating the exercise itself, you can evaluate how the organisation's crisis management structure functioned during the exercise.

The process can be assessed, with the critical processes serving as the point of departure. An assessment is made to see if the crisis management structure works as intended. The main focus here is on acting correctly. The outcomes can also be reviewed. Then, the emphasis is on the results delivered by the exercise process, i.e. primarily the efficiency and effectiveness of the measures taken.

To establish learning points and areas for improvement in terms of the crisis organisation, questions such as 'what happened' (describe), 'why did it happen?' (explain) and 'what does it tell us?' (analyse and reflect) can be asked during the evaluation. Lessons can be learned from the exercise in terms of how the exercise went and the effectiveness of the crisis management process, which will be the basis for improvements to the internal crisis management structure.

An observer can monitor the internal processes and incorporate their findings in the internal evaluation.

Evaluation points
Schedule a number of different evaluation points:
- **During the game:** During the game, players can be given a checklist/questionnaire so they can monitor their experiences immediately. This can be used to inform subsequent evaluation sessions, so the key evaluation points remain top-of-mind. Players can mention issues relating to the exercise itself as well as issues relating to the internal processes.
- **Immediately after the game:** Organise an afternoon evaluation session immediately after the game. If only one institution is involved in the exercise, you can discuss conclusions around the exercise itself and the internal processes. If multiple organisations are involved, it is a good idea to decide if you will evaluate the exercise itself only, or include the organisations' internal processes. Since content-related processes can be sensitive, it may be better to evaluate these internally only rather than in a group.
- **A few weeks after the game:** Meet with the exercise leadership (project group, programme group and steering group) to discuss how the exercise went and the results of the exercise.

Evaluation by participants

Depending on the room size where the evaluation sessions will take place, it is a good idea to indicate the maximum number of people who can take part in the evaluation in advance. In the case of OZON, the maximum was three participants from each institution. This always included the security officer who was part of the programme group, and one or two players.

Survey
As soon as the exercise is over, online questionnaires containing questions about the exercise process and/or questions about the achievement of the (internal) exercise objectives, own experiences, successful aspects of and learning points from the exercise can be sent to participants.

Appendix 17: Definitions

Term	Meaning
Master event list	A timeline on which interventions and actions are recorded. This serves as a guideline for the exercise.
Event	An event with general content. The number of events will depend on the objectives of the exercise. Various events are required in order to make the scenario realistic. [10]
Action	The consequences of an event. An action is intended to provoke a response from the participants. Participants must take action and make decisions on the basis of the events. The responses of the participants move the scenario forward.
Intervention	These are used to bring actions to participants' attention. Interventions include social media messages (e.g. Twitter), newspapers and media reports, phone calls from stakeholders, phone calls from journalists and emails from simulated contacts.
NO PLAY	During the course of the exercise, unforeseen circumstances may arise that prevent play from continuing. In this event, the exercise will be suspended. The rules that apply in this event are NO PLAY rules.
Lead In	A lead in explains the background to the scenario and outlines the current situation in the media and society. This information is reviewed prior to the exercise in order to ensure that everyone starts on an equal footing.
Sitrep	Situation report. A situation report contains information on the basis of which the situation can be assessed and a good overview of the situation can be obtained, and decisions such as upscaling can be taken.
Response cell	In the scenario, parties or people who are not actually involved in the exercise themselves often play a role, such as journalists, interest groups or other internal employees. In order to include these roles in the exercise, these parties are simulated by the response cell.

[10] ISO 22398:2013(E), Art. 5.2.14, p.18

Appendix 18: Checklist for organising a (cyber) crisis exercise based on the OZON model

Simulation exercise (Gold and Silver)

Phase 1: 3 weeks after kickoff / 37 weeks before the exercise
- ☐ Has a project group been set up?
- ☐ Have key objectives and exercise type been defined?
- ☐ Have the date and central location of the exercise been agreed on and documented?
- ☐ Has a budget been set?
- ☐ Has a name been set?
- ☐ Is there a wiki?
- ☐ Has the maximum number of participants been determined?
- ☐ Agree and announce deadline for applications
- ☐ Have the participants been invited?

Phase 2: 12 weeks after kickoff / 28 weeks before the exercise
- ☐ Have the participants registered?
- ☐ Has a programme group been set up?
- ☐ Has a steering group been set up?
- ☐ Have the dates of meetings been decided?
- ☐ Have you decided on and documented the dates of the evaluation(s) and the location?
- ☐ Have logistics and facilities such as lunch during the exercise been organised?

Phase 3: 13 weeks after kickoff / 26 weeks before the exercise
- ☐ Have the participants defined the objectives and scope of the exercise?
- ☐ Has a need/nice to have list been drawn up for the exercise scenario?

Phase 4: 16 weeks after kickoff / 24 weeks before the exercise
- ☐ Has a decision been made with regard to the closed system for distribution of media reports (emails or media simulator?)
- ☐ Has the central scenario been determined?
- ☐ Has it been decided what technical elements are required, and is it clear what needs to be purchased and/or built?
- ☐ Do you have a communication strategy and a communication plan?
- ☐ Is there a common press strategy?
- ☐ Decide whether you want to involve observers.

Phase 5: 27 weeks after kickoff / 13 weeks before the exercise
- ☐ Do you have an rough planning for each day of the exercise?
- ☐ Has the approximate institution-specific scenario been defined?

Phase 6: 35 weeks after kickoff / 5 weeks before the exercise
- ☐ If external parties are participating in the exercise, have they been invited?
- ☐ Has the central scenario been incorporated into the master event list?
- ☐ Have the institutions incorporated the scenarios into a master event list?
- ☐ Have all the central game elements/interventions been created?
- ☐ Have all the institution-specific elements/interventions been created?
- ☐ Have the technical elements/interventions been created?

- ☐ Has the documentation been created? For example:
  - ☐ Lead in
  - ☐ Information package for players

- ☐ Email to organisations
- ☐ Player briefing materials
- ☐ Player invitation email
- ☐ Address list
- ☐ Teasers, where appropriate

- ☐ Have the media for communication (email addresses/jabber et cetera) been activated and are they working?
- ☐ Have the observers been appointed?

- ☐ Have the technical resources been tested/distributed and are they working properly?
  - ☐ Raspberry Pi
  - ☐ Logfiles
  - ☐ Malware
  - ☐ Websites
  - ☐ Simulation environment that simulates the production environment

Phase 7: 38 weeks after kickoff / 2 weeks before the exercise
- ☐ Have the internal players been invited?
- ☐ Have the players been briefed?
- ☐ Have the response cells been briefed?
- ☐ Has the documentation been distributed among the players?
- ☐ Has the organisation been made aware that an exercise is about to take place?
- ☐ Have the press releases been prepared and press officers been instructed?

Phase 8: 39 weeks after kickoff / 1 week before the exercise
- ☐ Have all the interventions been incorporated into the closed media environment and are all the interventions ready for the exercise?

Phase 9: 40 weeks after kickoff / 0 weeks before the exercise
- ☐ Execution of exercise
- ☐ Hot wash evaluation

Phase 10: Between 0 and 4 weeks after the exercise
- ☐ Evaluate and process evaluation
- ☐ Communicate outcomes within the institution(s)

For the Capture the Flag exercise (Bronze exercise)
Additional points to consider if a Capture the Flag exercise will take place at the same time as the simulation exercise.

Phase 3: 13 weeks after kickoff / 27 weeks before the exercise
- ☐ Bronze exercise – Has an exercise planner been appointed at the Bronze institutions?

Phase 6: 35 weeks after kickoff / 5 weeks before the exercise
- ☐ Have the infiltrators been organised?
- ☐ Is the attack software for the Capture the Flag exercise ready?

Phase 7: 38 weeks after kickoff / 2 weeks before the exercise
- ☐ Do the infiltrators possess the infiltration software?
- ☐ Have the infiltrators been briefed on the tasks?
- ☐ Have the Bronze institutions been briefed on use of the media simulator/receipt of emails and on the Capture the Flag exercise?
- ☐ Have the infiltrators received a proof of exemption?