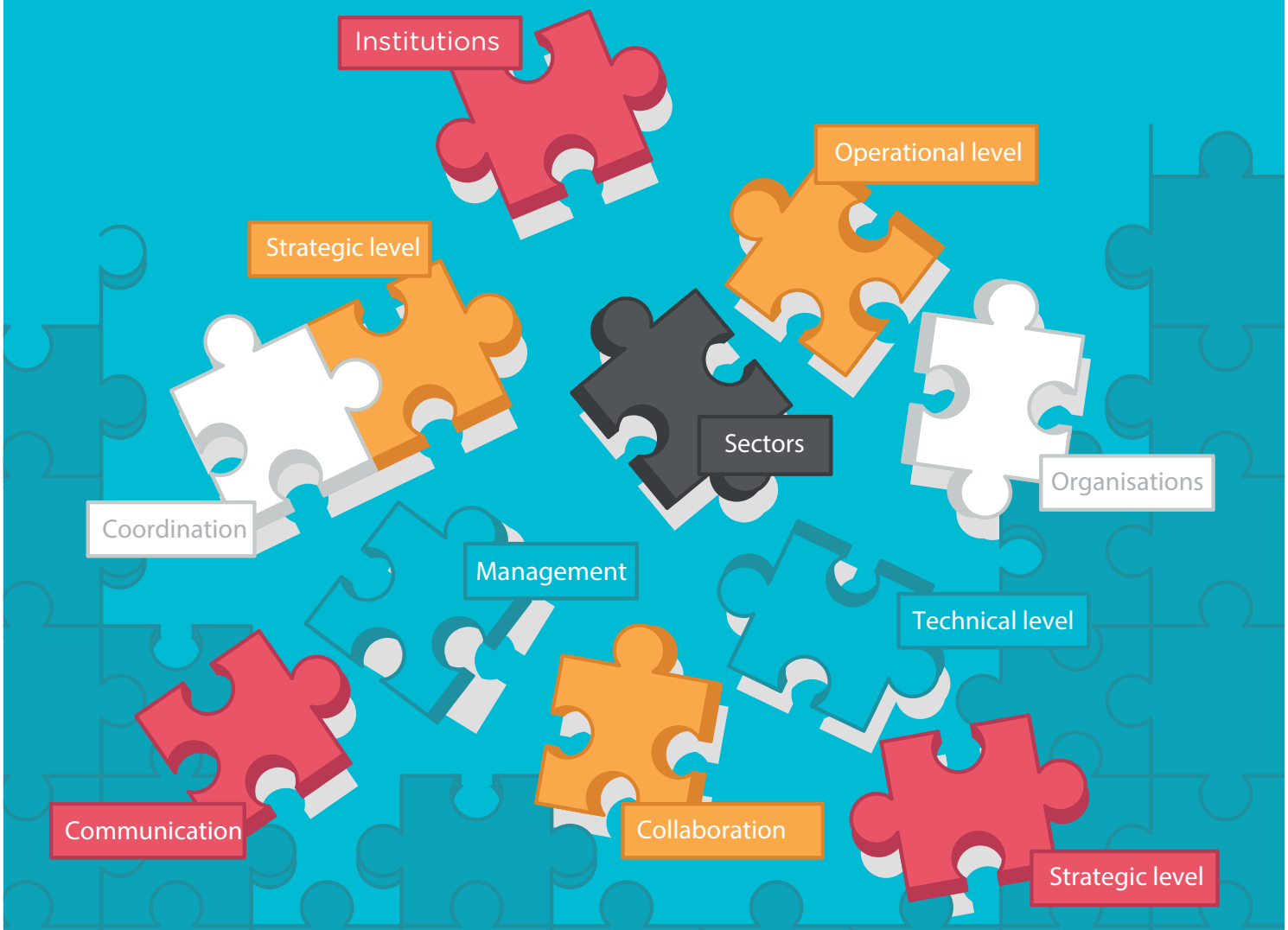
OZON CYBER CRISIS EXERCISE

A GAP-BRIDGING EXERCISE



SURF NET


Data Breach
Cyber Attack
System Safety

FOREWORD

The enthusiasm shown in the planning and execution of the OZON crisis exercise serves as clear proof that a major cyber crisis exercise is both necessary and useful. Cyber threats are very real: anybody can be affected by an incident at any time. OZON makes it possible to experience what a cyber crisis is like: to be ruthlessly targeted by a motivated hacker group. The institutions participating in the exercise were tested with a combination of technical attacks and moral dilemmas. This enabled us to thoroughly test all of our procedures, internal collaboration and escalation processes.

The aim of the exercise was to generate interest among technicians and involve management. The exercise met this objective with great success. I took part in the preparations and watched the exercise take shape with great pleasure. It is tremendously exciting for the organisation to see an exercise of this kind succeed, particularly when it is being carried out the first time and on such a wide scale. As Steering Committee members, we were not aware of the content of the exercise. This meant that I was able to play my own role in the exercise, which proved to be an extremely exciting and instructive experience.

OZON has enabled bridges to be built both within and between institutions. Crisis exercises that take different forms and scales are now a vital aspect of a security strategy designed to improve the resilience of institutions. Although we are not there yet as a sector, we are definitely on the right track. With OZON, we have made a significant step towards protecting our information infrastructure.

Maarten Brouwer
IT Director, Wageningen University and Research
Chairman, OZON Steering Committee

TABLE OF CONTENTS

1. INTRODUCTION

ICT and the Internet are becoming progressively indispensable, while analogue alternatives are disappearing. More and more, information is shared via the Internet and the education and research sector is not immune to these changes. As a result, ICT infrastructure - essential to institutions - is threatened to a much greater extent than before by the potential impact of cyber threats. In the education and research sector there is a lot of attention for threats to business continuity already, such as accidents or terrorist attacks. Cyber threats[1] can now be added.

Often, existing crisis management organisations are inadequately equipped to cope with a major cyber threat. To improve the organisation's resilience in the face of cyber threats, SURFnet organised a large-scale cyber crisis exercise in October 2016. The OZON Cyber Crisis Exercise was a SURFcert initiative in collaboration with SURFnet and 31 education and research institutions.

This whitepaper explains how to set up a cyber crisis exercise and demonstrates the importance of cyber crisis exercises for crisis management. Then it looks at how the OZON cyber crisis exercise was organised. Next, the outcomes and recommendations resulting from the OZON cyber crisis exercise are set out in detail. This whitepaper is intended for ICT policy makers and security specialists and can be used as a guide for organising an exercise.

Structure

Chapter 2 provides an insight into the background of crisis management. It begins with a definition of (cyber) incidents and (cyber) crises. Then we address how to deal with a crisis, with specific attention to the crisis plan. This section discusses various physical, social, and cyber risks with practical examples. We focus on cyber risks for education and research institutions that are relevant for the OZON cyber crisis exercise. The main actors, threats and vulnerabilities are also described.

Chapter 3 shows which exercises are possible for specific purposes and provides insight into the importance and the objectives of crisis exercises. This chapter gives some examples of cyber crisis exercises that were organised in the past.

Chapter 4 provides an overview of the organisation of a simulation exercise (such as the OZON cyber crisis exercise), and describes the three stages of a crisis exercise: preparation, execution and evaluation.

Finally, chapter 5 focuses on the OZON cyber crisis exercise itself. This chapter begins with how the exercise is organised. All aspects of the exercise are covered, including the scenario and what to take into consideration for the scenario, the different roles and tasks during the preparation phase, and the course taken by the exercise. Then, the results of the exercise are presented.

Chapter 6 concludes with recommendations for crisis management and the organisation of cyber crisis exercises.

[1] *Cyber is a broad term and includes interruption to, loss of and abuse of ICT. See https:// www.nctv.nl/organisatie/cs/index.aspx (consulted 20 October 2016).*

2. CRISIS MANAGEMENT

2.1 From incident to crisis

The education and research sector is prepared for various incidents. Most incidents are of an operational character and are dealt with by the line organisation, e.g. internal crisis management team, security or IT.

> *"An incident is an undesirable event, whether intentional or not, that has a negative impact on the quality of welfare, building and/or business processes and can be solved through daily procedures."*[2]

An incident can become a crisis:

> *"A crisis is an event that deeply interferes with the functioning of an organisation or a social system, and requires crucial decisions to be made quickly under pressure".*[3]

A crisis is likely to grow due to factors such as media attention and unrest among students, parents, patients, employees or society as a whole.

2.2 Dealing with a crisis

The impact of a crisis can be controlled with thorough preparation.[4] A coordinated approach is required in a crisis in order to direct and rationalise the decision-making process. It is important that tasks and roles are clear and that all concerned are able to react quickly. The threat, urgency and uncertainty are much greater in a crisis than in an incident, when there is usually sufficient time to react.

A crisis plan helps in the decision-making process, thereby avoiding unnecessary escalation. Most existing plans and procedures are focused on operational processes. Little attention is paid to strategy.[5] To indicate the need for strategic attention, it is important that the professional dealing with a crisis is on the agenda at board level and that specific arrangements are made.[6] A crisis plan includes preparing for a crisis and assessing how it is to be managed. The Ministry of Education encourages institutions to draw up and practise a crisis plan. This is part of the ministry's Integrated Higher Education Security programme.[7]

A coordinator can be designated to help shape the crisis management policy and the organisational form of the crisis plan. The crisis coordinator can draw up the crisis plan and assemble the crisis response teams during the preparation phase. They can also organise crisis exercises. To have a clear idea of the possible risks that may lead to a crisis, a risk assessment can be used to identify possible threats. Section 2.3 covers how to make an inventory of risks.

[2] *Based on http://www.bcmacademy.nl/nl/bcm-academy/informatie-over-het-vak/begrippenlijst and COT (2011). (consulted 10 October 2016).*
[3] *COT "Leren van incidenten" (2011), p. 37.*
[4] *http://www.integraalveilig-ho.nl/continuiteitmanagement/ (consulted 15 September 2016).*
[5] *COT "Elf Bouwstenen voor een Crisisplan" (2014) p. 2.*
[6] *http://crisismanagement.schoolenveiligheid.nl/algemeen/ (consulted 12 September 2016).*
[7] *www.integraalveilig-ho.nl (consulted 10 October 2016).*

Decision-making and coordination

During a crisis, clear decision-making and communication are vital. A large-scale crisis requires a crisis team that is able to coordinate and make decisions. An operational crisis team is usually assembled first of all to deal with operational issues. In a major crisis, it may be necessary to call on the expertise of a managerial crisis team. A managerial crisis team is necessary for issues of a more strategic nature. The tasks and responsibilities of the crisis teams are detailed in the crisis plan. Many decisions made at an operational level can have a strategic impact. It is extremely important to exchange information quickly and accurately. This information exchange may be organised according to a structure based on alerts and upscaling. When teams work actively together, the risk of exchanging conflicting messages what might impede the process, is avoided. Afterwards, it is also important to scale down the crisis. The resulting information will indicate whether the crisis was sufficiently controlled. Information analysed after the incident can be evaluated and formulated as lessons learned, which can then be applied within the organisation.[8]

External communication

Research and education institutions are increasingly receiving media attention during a crisis. This can put enormous pressure on institutions. Furthermore, internal and external stakeholders such as students and patients can put great pressure on institutions. Drawing up a press protocol and communication strategy helps to maintain the direction taken and facilitates communication with the press and stakeholders.

Training programmes can be deployed to ensure that members of the crisis team have the necessary knowledge and expertise. Regular exercise drills using crisis scenarios also improves the crisis team's skills.[9]

In April 2016, the working climate at the University of Utrecht received media attention from the daily evening newspaper, NRC Handelsblad. The report was quickly picked up by RTV Utrecht and other broadcasters. The Executive Board was forced to make a comment.[10]

2.3 Risks

A risk assessment provides insight into the potential security risks and their impact. Physical, social and cyber risks can result in a major crisis.[11] The greater the risk, the more chance the crisis threatens continuity. The level of threat depends on the specific characteristics of the institution, such as the occupants of the building, the location, size and business procedures. A threat can come from inside or outside the institution. Risks evolve, so it is a good idea to include a risk assessment in an annual Plan Do Check Act cycle.[12] It assesses how risks have developed, what this means for policy and which measures need to be taken as a result.[13]

[8] *COT "Elf Bouwstenen voor een Crisisplan" (2011), p. 12.*
[9] *COT "Leren van Incidenten" (2011), p. 12.*
[10] *http://www.rtvutrecht.nl/nieuws/1461998 (consulted 20 October 2016).*
[11] *See also http://www.integraalveilig-ho.nl/ for a general idea of the potential risks faced by higher education.*
[12] *Among others included in ISO 27001 for information security and ISO 22301 for business continuity.*
[13] *COT "Leren van Incidenten" (2011), p. 15.*

Some examples of physical security risks:
- fire
- accident
- disease
- terrorism
- failure of support services and processes (air conditioning)

Some examples of social security risks:
- fraud (exams, plagiarism)
- discrimination
- vandalism
- harassment
- aggression
- radicalisation[14]

In 2008, a dangerous fire destroyed the department of architectures building at the Delft University of Technology. Part of the complex collapsed. The fire was caused by a short circuit. When the fire started, there were 200-300 people in the building. Fortunately, there were no casualties.[15]

Cyberrisks

Business continuity management focuses on preventing future incidents and crises and having alternatives prepared in the form of plans and tools.[16] Contingency plans generally focus on measures to mitigate direct, visible and often physical damage. Far too little attention is paid to threats from cyber incidents and crises.

The SURF Cyber Risk Report 2015 cites the following cyber risks:[17]
- espionage
- acquisition and disclosure of data
- identity fraud
- ICT disruption
- manipulation of digital data storage
- control and misuse of ICT
- deliberate image defamation

2.4 From cyber incidents to a cyber crisis

> *A cyber incident is an IT incident that disrupts the expected availability of services and/or provokes the unauthorised disclosure, acquisition and/or modification of information.*[18]

A cyber incident, whether intentional or not, has a particular operational impact and simply requires a technical IT response. An incident usually has no long-term effects. Attention from the management team is not necessary and responsibility lies with the

[14] *Zannoni, Kuipers and Wensveen "Realisme in veiligheid en crisismanagement" (2012), p. 2.*
[15] *http://www.nu.nl/algemeen/1565130/brand-verwoest-faculteitsgebouw-bouwkunde-in-delft-video.html (consulted 20 October 2016).*
[16] *Zannoni, Kuipers and Wensveen "Realism in security and crisis management" (2012), p. 4.*
[17] *SURF Cyber Risk Report (2015), p. 27.*
[18] *ENISA, "Strategies for Incident Response and Cyber Crisis Cooperation" (2016), p. 105.*

ICT managers.[19] The difference between a cyber incident and other incidents is that cyber incidents can go undetected for a long time. The urgency and impact of the incident is not immediately evident.[20] As a result, a cyber incident can develop into a cyber crisis.

> *A cyber crisis is "an abnormal and unstable situation in which strategic goals, reputation and reliability are threatened by a disturbance, intentional or unintentional, at the core of the targeted organisation."*[21]

A cyber crisis has a much greater impact on the organisation than a cyber incident. The likely consequences of a cyber crisis are:
- loss of confidence (integrity),
- significant political and media attention (damage to reputation),
- loss of income (financial loss).[22]

In a cyber crisis, the consequences are not always clear, nor is the impact on business continuity. If a cyber crisis is underestimated, it can spread like wildfire and also affect other parties.[23]

2.5 Cyber threats to education and research institutions

Actors

The 2015 SURF Cyber Risk Report shows that the threat of students, staff, cyber criminals and cyber vandals are particularly relevant to the education and research sector.[24] Nationwide, the most important threats come from professional criminals and state actors. Hacktivists (politically or socially motivated hackers) are also a real threat.[25] As shown in the 2016 Cyber Security Report by the Dutch National Cyber Security Centrum (NCSC)[26], there is a growing threat from cyber vandals and script kiddies. Internal individual actors present in the organisation (temporarily or otherwise) may constitute, or may have constituted, a threat. This includes (former) employees, temporary staff, suppliers and students.[27]

Cyber threats

The SURF Cyber Risk Report[28] identifies cyber threats to education and research institutions.

- Institutions are increasingly targeted by **cyber espionage attacks** that aim to **obtain information** and/or to **make them public**.[29] **The manipulation of data** is a major threat to its integrity.[30] This creates a range of different dilemmas with regard to privacy and security.[31] When the integrity, reliability and confidentiality of such information is at stake, there is potential for significant damage.[32]

[19] *Zannoni "Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont" (2016).*
[20] *http://www.cot.nl/pdf/COT-Leren-van-Dorifel-15-januari-2013.pdf (consulted 12 September 2016).*
[21] *COT "concept scenariokaart Cyberaanval" (2016); see also ENISA "Report on cyber crisis cooperation and management" (2014).*
[22] *Zannoni "Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont" (2016).*
[23] *http://www.cot.nl/pdf/COT-Leren-van-Dorifel-15-januari-2013.pdf (consulted 12 September 2016).*
[24] *SURF Cyberdreigingsbeeld (2015), p. 18.*
[25] *SURF Cyberdreigingsbeeld (2015), p. 19.*
[26] *NCSC Cybersecuritybeeld Nederland (2016).*
[27] *NCSC Cybersecuritybeeld Nederland (2015), p. 30.*
[28] *SURF Cyberdreigingsbeeld (2015).*
[29] *NCSC Cybersecuritybeeld Nederland (2015), p. 23.*
[30] *This primarily refers to sensitive data from research into subjects such as chemistry, biology, radiology and nuclear science. See also NCSC Cybersecuritybeeld Nederland (2015), p. 19.*
[31] *SURF Cyberdreigingsbeeld (2015), p. 15.*
[32] *SURF Cyberdreigingsbeeld (2015), p. 18 features an overview of the different security aspects.*

- Education and research institutions are increasingly being threatened by **identity fraud**, which is cause for concern because students might abuse this to get a second attempt for an exam or stolen identities are used for malicious purposes such as spam or phishing.[33]
- The institution's **network** can also be **misused** for malicious purposes.[34] The open, stable and rapid ICT infrastructure of the Netherlands' universities and colleges is a good operating base for launching cyber attacks elsewhere. This can be detrimental to the reputation of educational institutions.[35]
- **ICT disruption**: DDoS attacks are common within the education and research sector. It is striking that peaks in activity are recorded immediately after school holidays, during exam periods and at the start of the school year.[36] Actively disrupting the ICT services has an impact on ongoing processes and is one way to cause harm. It is important that available systems and connections remain highly accessible, with interruptions kept to a minimum.[37] Otherwise, this can have severe consequences if essential systems are affected, such as hospital equipment.
- **Deliberate image defamation**: for example, damage to websites or hacking of social media accounts.[38]

Vulnerabilities

These threats occur when there are known vulnerabilities in terms of technology, processes or human elements.[39]

- **Access to technology** - Accessibility within education and research institutions is increasing.[40] Institutions are offering more and more courses, examinations and assignments via the Internet. More and more devices are interconnected and connected to the Internet remotely. This makes the network vulnerable to potential attacks.[41] Furthermore, students, researchers and teachers work off-campus more often and hence work online. This means that they take data from within the educational institution outside the institution's network. Traditional security at the network edges is no longer sufficient to secure data. As such, it is becoming increasingly important to secure the data and improve the organisation of access to data.[42] With more and more devices becoming connected, this increases the number of devices to be updated. It is not always easy to update systems and devices. Systems are complex in themselves or are dependent on hardware and other systems.[43]

- **Process** - Education and research institutions have to deal with increasing numbers of users who frequently exchange a rapidly growing quantity of data. Access to data and its usage must be well organised. This makes procedures for identity and access management essential. As such, education and research institutions are increasingly turning to cloud services.[44] Access to cloud services and data storage must therefore be as well protected as the company network.[45] A simple password is often not secure enough, or recovery capabilities are weak. Passwords can be easily changed or become obsolete. Users need to be more aware of security risks

[33] *SURF Cyberdreigingsbeeld (2015), p. 30.*
[34] *SURF Cyberdreigingsbeeld (2015), p. 32.*
[35] *SURF Cyberdreigingsbeeld (2015), p. 19.*
[36] *SURF Cyberdreigingsbeeld (2015), p. 39.*
[37] *SURF Cyberdreigingsbeeld (2015), p. 3.*
[38] *SURF Cyberdreigingsbeeld (2015), p. 27.*
[39] *SANS "People, Process, and Technologies Impact on Information Data Loss" (2012) and SURF Cyberdreigingsbeeld (2015), p. 19.*
[40] *ENISA Threat Landscape (2014). Examples include projectors, printers, laptops, landline and mobile phones, tablets, hospital equipment, building equipment and kitchen appliances.*
[41] *SURF Cyberdreigingsbeeld (2015), p. 16.*
[42] *SURF Cyberdreigingsbeeld (2015), p. 14.*
[43] *Idem.*
[44] *SURF Cyberdreigingsbeeld (2015), p. 6.*
[45] *Idem.*

when creating passwords. Service providers should perform better checks when changing passwords. The use of safer login methods such as multifactor authentication helps to solve the password dilemma. The risk of espionage or violation of privacy laws is increasing due to the fact that many cloud storage services are located outside the Netherlands.[46] The legal standards framework for higher education ("Juridisch Normenkader (Cloud)services")[47] describes the standards regarding conditions for access, security and international aspects for cloud services. These can be used as the basis for contracts with cloud providers.

- **User** - The user plays an important role in the use of technology and processes. It is becoming more and more frequent for students and staff to use weak passwords, insecure devices such as USB sticks or insufficiently secure cloud services. Users often fail to update their computers and mobile devices regularly due to difficulties. Many users often use outdated versions of soft- and hardware as well. Spear phishing[48] is another growing threat, because simulated emails are almost indistinguishable from real ones. Furthermore, social engineering is still popular and successful particularly for specific activities. People are increasingly mixing professional and private use, making it difficult, for example, for organisations to stop phishing through email filtering.[49] In practice, it is difficult to convey general skills to users. Practice is the most effective way of communicating with users, starting with a clear and realistic problem.[50]

Targeted attacks on education and research institutions

Attackers exploit the vulnerabilities of the education and research sector. Most attacks use spear phishing to obtain sensitive data. The distribution of phishing emails is a sophisticated cyber attack tactic, as they can almost never be distinguished from real emails anymore.[51] The mails are focused on one or a limited group of persons within an organisation.

They are used to identify specific information in order to gain access to the organisations' internal networks. One example of spear phishing is CEO/CFO fraud, when an attacker sends an email pretending to be the CEO or CFO of the company. However, use of methods to identify the authenticity of emails[52] is rare. Spreading malware via infected websites or emails is called a watering hole attack.[53]

More frequently, cyber criminals are using methods over a long period of time. This is sometimes referred to as Advanced Persistent Threats (APTs). They are difficult to detect because they often bypass existing security measures. Through Remote Access Tools (RATs), it is possible to take over many functions from the general user.[54] They often focus their attacks on administrators, researchers and directors of education and research institutions.[55] Actors rarely focus on one organisation at a time, preferring instead to attack dozens of public and/or private organisations simultaneously.

[46] *NCSC Cybersecuritybeeld Nederland (2015), p. 5.*
[47] *SURF Juridisch Normenkader (Cloud)services 2016 - consulted via https://www.surf.nl/kennis-bank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html on 16 November 2016.*
[48] *Spear phishing is a sophisticated cyber attack method using phishing emails which are distributed to one or more specific persons.*
[49] *NCSC Cybersecuritybeeld Nederland (2015), p. 43.*
[50] *NCSC Cybersecuritybeeld Nederland (2015), p. 10.*
[51] *The attackers "fish" for login information and other user data.*
[52] *This includes: digital signatures, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).*
[53] *These are called watering hole attacks. See also NCSC Cybersecuritybeeld Nederland (2015), p. 43.*
[54] *NCSC Cybersecuritybeeld Nederland (2015), p. 41.*
[55] *SURF Cyberdreigingsbeeld (2015), p. 16.*

In 2015, 7,000 students were sent phishing emails, supposedly from Inholland, trying to retrieve student records.[56] Health care institutions are also being targeted by spear phishing more and more frequently as medical records become increasingly attractive to cybercriminals.[57]

Impact

A crisis can have a major impact on the organisation (organisation, research and operations[58]) and may cause financial losses through reduced income, deterioration of integrity and loss of trust. It might also cause reputation damage due to the negative attention given by stakeholders, politicians and the media to the crisis. Sometimes a crisis can even lead to loss of life.[59] A crisis often causes more than one form of damage.

- **Services** - Failure of IT systems and processes are the primary cause of major disruption to services. For example, interruptions to critical ICT systems and medical devices in hospitals can have fatal consequences for patients. Failure of education and research systems can have implications for operational performance: cancellation of lessons or exams, and postponed or repeated research.

In 2013, ROC West Brabant Breda North experienced the adverse effects of a network failure on its services. Its network was barely operational for weeks because a student had shut it down through DDoS Attacks.[60]

- **Financial impact** - The economic impact of a cyber crisis is usually severe. Research institutions often possess highly sensitive data, and loss and disclosure can lead to substantial liability claims. As a result, students may decide to study elsewhere, research funding from bodies such as the Netherlands Organisation for Scientific Research (NWO) may be lost, and research contracts may be awarded to other institutions.[61] If sensitive company information is made public, it can have a direct influence on competitiveness and result in claims for damages. The distribution of unpublished research can reduce competitiveness. A bad reputation in the educational process can have a negative impact on enrolment figures. This has a knock-on effect in terms of finance. Crypto/ransomware can also be very costly. In addition to paying the high costs for criminal activity, there are significant costs associated with the unavailability of the network and necessary repairs.

[56] *http://www.at5.nl/artikelen/148428/waarschuwing_voor_phishingmail_inholland (consulted 20 October 2016).*
[57] *NCSC Cybersecuritybeeld Nederland (2015), p. 76.*
[58] *SURF Cyberdreigingsbeeld (2015), p. 19.*
[59] *Zannoni "Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont" (2016).*
[60] *http://www.nu.nl/tech/3627406/16-jarige-jongen-opgepakt-cyberaanval-school.html (consulted 16 October 2016).*
[61] *SURF Cyberdreigingsbeeld (2015), p. 28.*

In 2015, the Vrije Universiteit Amsterdam was the victim of ransomware.[62] Around 200 computers were infected. Malware was spread via email attachments. The impact was limited thanks to satisfactory backups, so the amount demanded by the hackers did not have to be paid. Damages amounted to an estimated EUR 154,000.[63] In June 2016, a university in Canada paid the sum of CAD 20,000 in order to retrieve access to emails and files.[64]

- **Loss of confidence and damage to reputation** - When a cyber crisis appears, individual, organisational and societal interests are often affected. When sensitive information about the institution or others goes public, confidence in the institution is diminished and its image is damaged. People risk losing confidence in an institution if they are worried about data leaks, privacy safeguards and insufficient ICT service availability. They are likely to use ICT services less frequently or opt for an alternative.[65] This can cause limitations to economic growth and innovative development.

A crisis of this kind occurred in June 2016 when a leak was found in the information system of the University of Amsterdam (UvA) and the Hogeschool van Amsterdam (HvA), which made the data of 385,000 HvA and 237,000 UvA students public. Students had access to this data through part of the system that was no longer used, but was still accessible.[66]

In 2011, student hackers from Thorbecke Lyceum in Rotterdam were caught systematically adjusting grades. They would do this for other students for a fee. They were able to do this because they had acquired the tutors' passwords. In 2014, something similar happened at Barlaeus Lyceum in Amsterdam, where students had access to the school's registration system for the entire year. They increased grades and deleted messages from absentees.[67]

In 2012, dozens of medical records and the data of 493,000 patients at Groene Hart Hospital in Gouda were on a server that had virtually no security. The data was subsequently made available over the Internet.[68]

Increasing resilience

If resilience is to be increased, an organisation's weak spots and threats to the organisation have to be identified. A risk assessment is an effective way of doing this. As all of the conditions are changing constantly, this requires a structured approach, e.g. by creating a security management process. It is recommended to join forces with other security services and establish a comprehensive security policy.

[62] *http://infosecuritymagazine.nl/2015/03/11/vrije-universiteit-amsterdam-besmet-met-ransomware/ (consulted 16 October 2016)*
[63] *SURF Cyberdreigingsbeeld (2015) p. 28.*
[64] *http://www.bbc.com/news/technology-36478650 (consulted 16 October 2016)*
[65] *NCSC Cybersecuritybeeld Nederland (2015), p. 52.*
[66] *http://www.nu.nl/internet/4280591/studentgegevens-uva-en-hva-waren-makkelijk-vindbaar-systeemlek.html (consulted 16 October 2016)*
[67] *http://www.nu.nl/internet/2427939/hackende-scholieren-betrapt-cijferfraude.html and http://www.nu.nl/binnenland/3931116/cijferfraude-leerlingen-amsterdams-gymnasium.html (consulted 16 October 2016)*
[68] *http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html (consulted 16 October 2016)*

- **Security management** - The information security management system protects the confidentiality, integrity and availability of information through a risk management process. A system of this kind also assures stakeholders that risks are managed appropriately.[69] One element of security management is to identify the organisation's valuable "assets"[70]. It identifies the threats faced by those assets and how they can best be protected. The organisation defines the tasks and responsibilities in advance. Protection measures include policy and operational measures that are maintained and evaluated periodically. A crisis exercise is the ultimate test for evaluating the effectiveness of the measures taken to protect an organisation's assets.

- **Risk management** – Institutions carry out risk assessments in order to analyse existing threats. A risk inventory and assessment enables the risks to be identified immediately. Risk management means that institutions purposefully implement security measures as an integral part of their business operations.[71] It is important to have an understanding of potential cyber risks that could create a crisis.[72] Cyber risks are constantly changing. SURFnet therefore draws up an annual Cyber Risk Report[73] for the education and research sector. Institutions can use this report to reassess the risks each year and to set up the appropriate crisis plan accordingly. Having insight into the possible risks means that they can be swiftly detected and addressed.

- **Cyber element of a crisis plan** – Because a cyber crisis requires both operational and strategic measures, it is important that information is shared to allow for timely decisions to be made. The crisis plan includes appropriate protocols, so that the IT department can react promptly and escalate to a strategic level if necessary. It is also useful if the IT department is part of the crisis team. The topic of cyber security has to be an integral part of the crisis management plan.

- **Awareness** – Human error can be prevented by increasing user awareness. Users take a safer approach when they understand the consequences of their actions. This is why different campaigns such as "CyberSafe Yourself"[74] are set up to increase awareness.

- **Operational measures** – Awareness is not always enough. Other measures are taken to increase resilience against crises.[75] Multifactor authentication is required to reduce the risk of malicious and other unauthorised usage of passwords and usernames.[76] Organisations are also increasingly encrypting data when storing and transmitting it.

[69] *ISO 27001:2013 Information Security Management, Oct. 2013.*
[70] *Physical and logical: knowledge and information.*
[71] *NCSC Cybersecuritybeeld Nederland (2015), p. 12.*
[72] *See section on cyber risks.*
[73] *https://www.surf.nl/persberichten/2015/12/surf-publiceert-cyberdreigingsbeeld-2015.html (consulted 15 October 2016)*
[74] *https://www.cybersaveyourself.nl/ see also: https://www.surf.nl/diensten-en-producten/cybersave-yourself/index.html (consulted 10 October 2016)*
[75] *Examples include DKIM, SPF and DMARC.*
[76] *Such as the previously described methods (spear phishing and APTs)*

Cooperation within and between institutions

In today's digital society, ICT structures are closely interlinked. As there is extensive connectivity within the education and research sector and institutions exchange large amounts of data, cyber crises often affect more than one organisation. A cyber crisis may sometimes even be sector-wide or cross-sectoral. As such, cyber risks cannot be tackled by a single organisation alone. Working together is vital.

It is also important to have the requisite knowledge to properly tackle a crisis. When organisations share knowledge with one other, it takes less effort to gain a more complete picture of the situation. By working together, they can react more quickly and work together to provide an adequate response. In addition, working together ensures that organisations have a better understanding of how to respond to a cyber crisis. Both national and international organisations are increasingly seeking cooperation.[77]

Practicing with cyber crisis scenarios

Practicing cyber crisis scenarios teaches institutions how to respond in the event of a crisis. More and more cyber crisis exercises are being organised in different sectors.[78] Conducting such exercises teaches employees and organisations what they can and must do when confronted with a cyber crisis.[79] They also learn from each other, which is equally valuable.

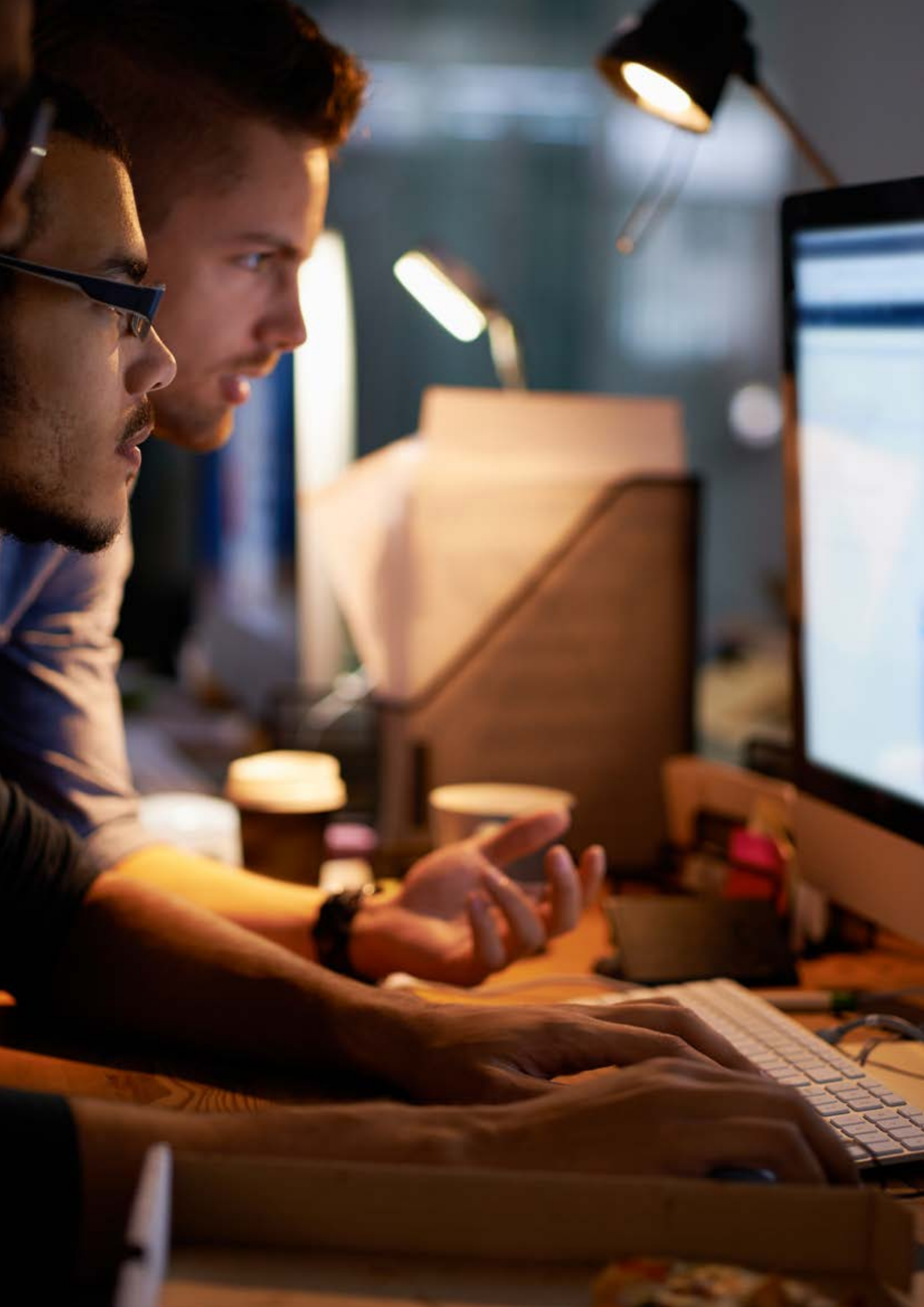
2.6 Conclusion

If an institution is not sufficiently resilient, malevolent actors can exploit its vulnerabilities, leaving the institution open to abuse and other risks. The interests of the institutions and other parties may be endangered.
To cope with threats, the institution needs to make sure that it is resilient over the long term. It is essential that the parties concerned are aware of the risks and the skills needed to be able to defend the institution against an attack. Operational and strategic measures are also essential. One strategic measure for an institution to increase its resilience is to make cyber security part of the general crisis approach.

SURFnet plays an active role in improving resilience against cyber threats and contributes to the cooperation between education and research institutions. This includes the drafting of an annual sector-specific cyber risk report. Cyber crisis practise is a new resource. Practising such exercises provides an additional base for cyber security at management level.
This is especially true for cyber risks that can cause a major cyber crisis, including damage to reputation. A crisis of this kind cannot be solved through technical measures alone. It has been shown in the past that such scenarios are realistic.

In October 2016, SURFnet organized the first OZON Cyber Crisis Exercise to help member institutions increase their resilience against cyber threats. Before going into the details of the OZON cyber crisis exercise, the types and backgrounds of crisis exercises in general are covered.

[77] *Examples include collaborations between banks at national and international level and within the international telecommunications industry. See ENISA "On national and International Cyber Exercises" (2012), p. 2.*
[78] *Examples include: ENISA's Cyber Europe (European) exercise took place on 13 and 14 October 2016; ISIDOOR, organised by NCTV (national), took place in June 2015; CyberDawn was organised for the telecommunications sector (national) in October 2014.*
[79] *NCSC Cybersecuritybeeld Nederland (2015), p. 52.*



3. CRISIS EXERCISES

3.1 Introduction

An organisation's resilience to a crisis is improved by practising with a crisis scenario. Drills and practice exercises are common for social and physical security risks. Cyber threats are a growing risk. General procedures for other crisis exercises can be applied to cyber crisis exercises. This chapter therefore discusses the general background of crisis exercises and then takes a look at specific cyber crisis exercises.

3.2 The importance of such exercises

Practising crisis scenarios make employees aware of potential risks. It is important to train these skills, because employees often have to make decisions under pressure. Furthermore, crisis structures can be assessed against reality (whether fictional or not). This indicates whether the crisis structure is well organised and whether people know how to contact each other. Another positive effect of practising crisis scenarios is that members of the crisis management team get to know each other better under crisis conditions.[80] Exercises improve both internal and external collaboration. This means employees act more quickly and effectively in a real crisis. Furthermore, lessons learned from the exercise can be used to improve crisis management.[81]

3.3 Exercise goals

One of the first steps in organising an exercise is to determine the purpose of the exercise; this determines the execution and evaluation of the exercise. The ISO guidelines for crisis exercises have five main goals: investigation, testing, training, cooperation and experimentation.[82]

1. **Investigation** involves an initial exploration of a crisis or cooperation with relevant parties. The focus is on the content (crisis-specific) or more general issues (collaboration and communication).[83]

2. **Testing** participants' skills and evaluating the organisation and systems enables the focus to be placed on critical processes such as issuing reports and alerts, upscaling, information management, and leadership and coordination. This aspect involves testing whether the crisis organisation is prepared in the event of a crisis.[84]

3. **Training** is about coaching, learning and development of individual skills. This contributes to improved individual knowledge and insight.[85] [86] [87] Participants can then apply what they have learnt to the organisation.

[80] *http://www.cot.nl/w/Artikel-COT-in-Magazine-Nationale-Veiligheid.pdf (consulted 12 September 2016)*
[81] *ENISA "On national and International Cyber Exercises" (2012), p. 7.*
[82] *ISO 22398:2013 Social Security - Guidelines for exercises, Sept 2013, p. v.*
[83] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013), p. 7.*
[84] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013), p. 7.*
[85] *Idem*
[86] *ISO 22398:2013 Social Security - Guidelines for exercises, Sept 2013.*
[87] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 17.*

4. Through cooperation, people and organisations have the opportunity to learn to work together towards a common goal and achieve a joint result.[88]

5. Through experimentation, participants try out new methods and/or procedures with the aim of refining existing methods and procedures.[89]

Exercise objectives at organisational level

Specific, targeted organisational exercise objectives are formulated based on the above primary objectives. The most common sub-goals in a crisis exercise are: testing procedures, decision-making, critical processes, internal and external communication, training participants and gaining experience. For cyber security exercises, the focus is often on testing and developing skills, training participants and gaining knowledge.[90]

Organisations can formulate sub-goals based on the primary objectives. Common sub-goals are: [91]

Procedures and assessments
- Identifying and applying plans, procedures, processes and structures
- Gaining an overview and making an assessment and decisions

Internal and external communication
- Adapting and communicating
- Crisis communication
- Collaboration
- Teamwork

Critical processes
- Alerts and escalation
- Information management
- Leadership and coordination

Experience
- Gaining experience and becoming proficient

3.4 Forms of crisis exercises

There are different forms of crisis exercise. The purpose of the exercise determines which type of crisis exercise is suitable. Each type has its own formats, methods, costs and benefits.

Crisis exercises can be divided into two types:

1. **Discussion-based exercises**[92] to familiarise participants with plans, policies and procedures. In discussion-based exercises, participants discuss a specific, predefined dilemma.

2. **Practical exercises** are used to test plans, policies and procedures, and train employees. A simulation that correlates with the real environment is usually chosen.[93]

[88] *ISO 22398:2013 Social Security - Guidelines for exercises, Sept 2013, p. v.*
[89] *ISO 22398:2013 Social Security - Guidelines for exercises, Sept 2013, p. v.*
[90] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 17.*
[91] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, (2013), p. 19.*
[92] *ISO 22398:2013 also refers to them as "dilemma exercises"; art. 5.2.13, p. 16.*
[93] *ISO 22398:2013, art. 5.2.13, p. 16.*

Examples of discussion-based exercises[94]

- **Desk Check** – A desk check is a method used to validate plans and procedures and any changes to them. This is usually conducted in conversation with the author of the plans and procedures. The plans and procedures based on the scenario are discussed step by step. This makes it clear what steps are needed and how they should be executed.[95]

- **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 specific steps of the crisis are dealt with, including detection, escalation, response, follow-up and conclusion of the situation. A walkthrough lasts half a day on average.[96] A walkthrough can be practised either internally or with other partners who have a role in the crisis.

- **Workshop** – Working through a scenario step by step; participants also discuss the various responses and actions. This makes it possible to rehearse the responses and actions of teams and individual participants without time pressure. This helps to improve coping skills for crisis situations and scenarios.

- **Tabletop exercise** – a tabletop exercise covers all aspects of crisis management. All participants receive the same information in advance about the simulated crisis situation and their role. During the exercise, players can use simulated media messages. Through the tabletop, the crisis team can share relevant information, gain an overview, make (suitable) decisions and take (communication) measures.[97] A tabletop exercise is a good solution for developing the crisis structure in a relatively calm environment and practising cooperation and/or training in specific skills. A tabletop exercise is a good option even if an organisation has not yet conducted an interactive simulation exercise.

Examples of practical exercises

- **Comms check** – A comms check (call exercise) is used to check and validate communication methods and notification systems. This sort of exercise is used to check the systems and infrastructure and to test whether they all function correctly.[98]

- **Distributed tabletop exercise** – A distributed tabletop is a role-play exercise where participants play their usual role in the plans and procedures of a scenario.[99] This exercise is similar in structure to a tabletop exercise, but there is no possibility for discussion. Participants must act as though there really is a crisis. Possible reactions can be discussed later in an evaluation. The advantage of this exercise is that participants can practise procedures and actions in a routine environment.

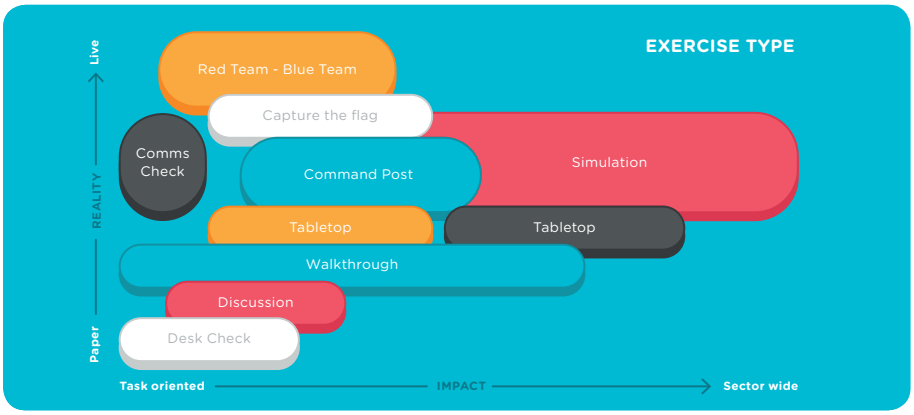
- **Command Post Exercise (CPX)**[100] – In a CPX (sandbox exercise), a crisis is simulated without the use of emergency services, external environmental factors or players. The crisis teams deal with questions and orders in a realistic and evolving scenario. As a result, teams respond to an evolving scenario exercise in their own environment, with their own facilities, actions and responses.[101]

[94] *This can also be computer-based.*
[95] *ENISA "On national and International Cyber Exercises" (2012), p. 15.*
[96] *http://www.cot.nl/crisismanagement/crisisoefeningen/walkthrough/ (consulted on 5 September 2016)*
[97] *http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ (consulted on 5 September 2016)*
[98] *ENISA "On national and International Cyber Exercises" (2012), p. 15.*
[99] *Idem.*
[100] *http://www.pm.be/oefeningen_op_maat/command_post_exercise.html (consulted on 12 September 2016)*
[101] *ENISA "On national and International Cyber Exercises" (2012), p. 15.*

- **Simulation Exercise** – In a simulation exercise, participants play out a realistic scenario in their own environment. Participants practise under normal circumstances insofar as is possible, with their own resources in their own environment. The rest of the scenario develops as a result of their decisions and actions. A simulation exercise is suitable if the aim of the exercise is to test and train participants under pressure in their own environment. [102] The intensity and the development of the scenario depend on the number of participants and their level of experience. It is also important to decide whether only will internal parties participate or whether external parties will also be included. A simulation exercise can last 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 element and "capture" it. This can be conducted in teams or individually, and in competition or not. In a cyber-related capture the flag, the aim is often to detect and catch simulated hackers who target 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 attempt. This exercise increases the awareness of possible risks. The exercise also gives insight into possible vulnerabilities and methods for dealing with them. The exercise also gives insight into strategies for detecting an attack and how to react. [103]



Gap-bridging exercise

Crisis exercises can build bridges between the tactical/operational level and strategic level, and/or between technical and non-technical operators. In an exercise of this nature, the capacity of the operational crisis team to escalate to the strategic crisis team is tested and trained, and mutual cooperation is encouraged. For this purpose, the scenario can be tailored specifically to a crisis situation with dilemmas at both operational and strategic level for which it is only possible to find a solution by working together. In addition to internal collaboration, an exercise can be cross-organisational and/or cross-sectoral.

3.5 Cyber crisis exercise

Practising cyber security scenarios has been attracting more and more attention in recent years. In its 2009 statement, "Critical information infrastructure Protection COM (2009) - 149", the European Commission invited member states to organise *"regular cyber crisis exercises for organising a response to large-scale network*

[102] http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ *(consulted on 5 September 2016)*
[103] https://www.encs.eu/wp-content/uploads/2015/08/2015_ENCS_Factsheet_RedBlue_Training_v1.pdf *(consulted 20 Oktober 2016) This form of exercise is used in various sectors, including ICT, defence and energy.*

security incidents and subsequent recovery".[104] In COM (2011) – 163, the European Commission once again underlined the importance of cyber crisis exercises.

> *"There is a broad consensus that cyber crisis exercises help to enhance the preparedness, response and knowledge of stakeholders in reacting to cyber incidents."*[105]

Practising a cyber scenario is an important tool for testing crisis management and communication structures. Furthermore, exercises contribute to defining and increasing the resilience of an organisation against cyber crises, ICT technical defects and incidents involving critical information structures. Cyber crisis exercises help to build bridges between the tactical/operational level and the strategic level. Stakeholders involved in a crisis often do not work together or even communicate with one other. This is because they do not usually cross paths in daily operations and are focused on their own organisational responsibilities[106]. Exercises help to improve collaboration both within and between organisations.

Examples of cyber crisis exercises

- In the same month as the SURFnet OZON cyber crisis exercise, ENISA organised its biannual cyber security exercise: **Cyber Europe 2016**.[107] Several thousand experts from 28 EU member states, Switzerland and Norway participated in the exercise. The scenario was developed at the operational and technical level from April 2016 and reached a climax on 13 and 14 October. The scenario threatened to have a major impact on the unity of the digital market. The motto of the exercise was "Stronger together." Cooperation at all levels was required to successfully anticipate a large, cross-border cyber crisis. It was the first time a simulation was used.

- In 2012, during **Cyber Europe 2012**, 300 cyber security professionals from 25 countries participated in a tabletop exercise organised by ENISA. This was an exercise on a national level. The NCSC was the primary contact for the Netherlands.[108]

- In 2014, the NCSC and Cert Bund organised a tabletop exercise to develop cooperation between Germany and the Netherlands with regard to cyber crisis management.[109]

- In October 2014, the Dutch telecommunications sector held its first large-scale cyber security exercise, **CyberDawn**.[110] The aim was to test cooperation between the public sector and private partners in other vital sectors in the event of a major cyber incident.

- In June 2015, the NCTV, together with thirty public and private partners, organised a national operational cyber simulation exercise, **ISIDOOR**. During the exercise, the participants simulated cyber incidents, and data leaks and system vulnerabilities were identified. The government had to work with public and private parties to make decisions about the operational response to this incident.[111] SURFcert took part in the exercise.

[104] *ENISA "On national and International Cyber Exercises" (2012), p. 7.*
[105] *ENISA "On national and International Cyber Exercises" (2012), p. 2.*
[106] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 25.*
[107] *https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 (consulted on 21 October 2016)*
[108] *https://www.ncsc.nl/actueel/nieuwsberichten/internationale-oefening-cyber-europe-2012.html (consulted on 15 September 2016); The first exercise, Cyber Europe 2010, was organised by ENISA on 4 November 2010.*
[109] *https://www.ncsc.nl/actueel/nieuwsberichten/duits---nederlandse-oefening.html (consulted on 20 October 2016)*
[110] *https://www.nederlandict.nl/news/telecomsector-bouwt-met-grootschalige-oefening-cyberdawn-aan-sterke-samenwerking-op-cyber-security/ (consulted on 20 October 2016)*
[111] *See www.ncsc.nl; the NCSC (National Cyber Security Centre) helps to increase the collective resilience of the Dutch digital environment and thus promote a safe, open and stable information community by providing knowledge and perspectives for action.*

- **Cyberlympics**, the annual international 'capture the flag' contest, was a success, especially in terms of participation from "incident response teams" employed by large service providers. In 2013, the Netherlands won gold, silver and bronze at the World Cup thanks to the teams from Deloitte and KPN.[112]

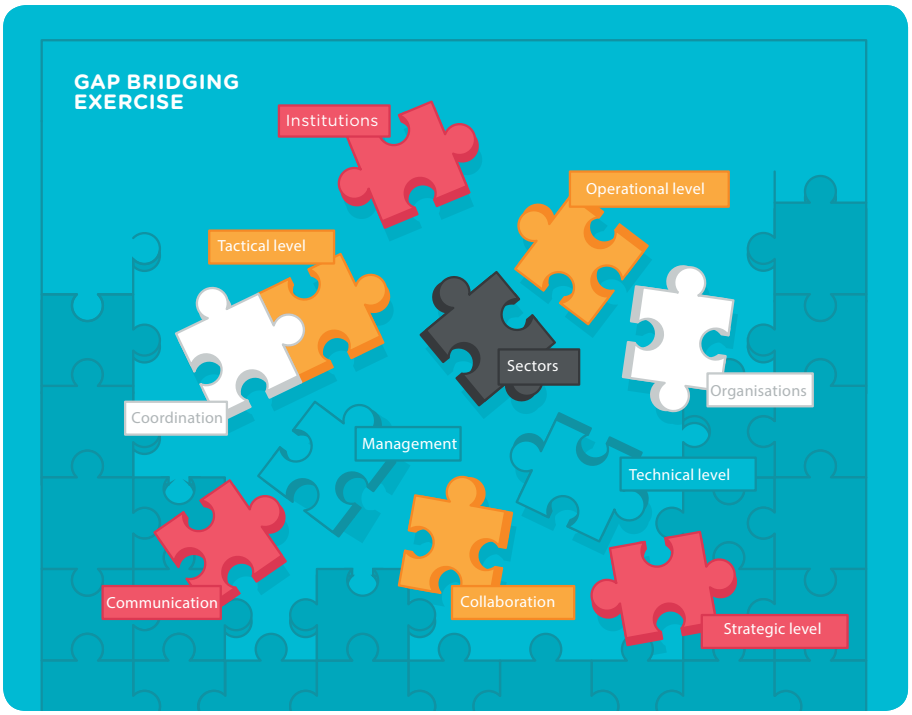
3.6 Conclusion

The application of cyber security exercises is still at an exploratory stage.[113] While there are indeed some positive examples of cyber crisis exercises, they are rarely held in practice. Many organisations have no clearly defined crisis structures that focus on cyber crises. Practice can help give form to these structures. Exploring the collaboration between stakeholders was an important objective in exercises such as Cyber Europe (international) and Cyber Dawn (national).

Even if the goals are not achieved in full, the exercise can still be successful because it sheds light on weaknesses.[114] The process and the results can expose knowledge gaps and make the participants aware of their own actions during a crisis.

An exercise will be unsuccessful if it is not well planned. However, a crisis exercise does not need a complicated structure in order to be useful. Each exercise contributes to developing the crisis management structure, learning to deal with a crisis and increasing awareness.[115]

A crisis exercise can be used to build bridges between the different levels (technical/operational and strategic level) and between different organisations or even between stakeholders across an entire sector. A cyber crisis exercise is a gap-bridging exercise.



[112] http://webwereld.nl/security/79360-nederland-wint-goud--zilver-en-brons-op-wk-ethisch-hacken (consulted on 21 October 2016)
[113] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 25.
[114] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 28.
[115] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 29.

4. ORGANISING A SIMULATION EXERCISE

Tabletop and simulation exercises are the most frequently implemented forms of cyber security exercises.[116] This chapter explains how to organise a simulation exercise, such as the OZON Cyber Crisis Exercise. Organising a crisis exercise is divided into three stages: preparation, execution and evaluation.[117]

4.1 Preparation

The goals of the exercise are established in the preparation stage. This defines the type of exercise that will be executed. The form of the exercise largely determines the content and planning of the preparation.

Project team

One or more project teams prepare the exercise. Team members in each project team fulfil different roles. For the central organisation and coordination of the exercise, it is advisable to form a project team with a project manager, project secretary, communications officer, project members and an observer.[118] The project manager is responsible for the planning and execution of the exercise. The project team is responsible for the scenario, documentation, logistics and evaluation.[119]

When several organisations are participating, it is recommended to create a programme group alongside the project team with a representative member from each participating organisation. For a complex exercise involving multiple participants, it is also recommended to create a Steering Committee for strategic decisions.

Schedule

The schedule depends on the complexity (operational/tactical/strategic), scope and resources available. In the case of participating institutions with busy agendas, it is helpful to schedule meeting times in advance. Most of the time is spent on the design and execution of the scenario. It is recommended to establish the plan in a full scenario in advance.

The plan includes:
- date and time of exercise
- duration of the exercise
- holiday periods
- preparation of the scenario
- preparation of technical and strategic evidence for the scenario
- participants' invitations, memos and letters
- evaluation

Conditions for the exercise

- **The duration of the exercise** depends on the exercise objectives, availability of participants and impact on the organisation (e.g. holidays). The duration can range from a few hours to a few days.

[116] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 17.*
[117] *Set out in ISO 22398:2013(E)*
[118] *ISO 22398:2013(E), art. 5.2.4.1, p. 10.*
[119] *ISO 22398:2013(E), art. 5.2.1, p. 8.*

- The impact on ongoing processes within the organisation should be minimised – as should the impact on existing infrastructure – in order to limit disruption to daily operations.
- It is necessary to have specific knowledge of the organisation to create the scenario. Hence, it is worth determining who has this knowledge, so that the preparation team can be assembled accordingly. Those who prepare the exercise cannot participate in the exercise itself; this must be taken into account.
- To avoid an exercise scenario being perceived as a real crisis, additional measures must be taken for it be to an exercise of closed nature. An established "closed" address book of participants and a closed environment for distributing messages ensures there is no confusion between the exercise and reality. Only the participants have access to this list. If a person is not in the address list, the response cell (this term is explained in Section 4.2) should be contacted.

Game rules

Rules are essential for an exercise to run smoothly. Some important rules include:

- All communications during the game will be provided with a code word to indicate that this is a drill. This is to avoid confusion between reality and the simulation.
- The project leader can call "NO PLAY" to stop the exercise (temporarily or permanently) if required, e.g. in the event of a real crisis that requires attention.[120]
- To mimic daily operations as closely as possible, participants use their usual means of communication.
- A "closed" address book is used to ensure the restricted nature of the exercise.

Drafting the scenario

The scenario is the basis of the exercise. It will have the desired impact it if corresponds to the reality in which participants identify themselves. Participants will be drawn into the crisis more quickly and will therefore react to the crisis realistically. It is recommended to make an inventory of crises that would be realistic within the organisations and that could be used as the basis for the exercise scenario. The scenario should not be too complex to ensure that participants are not overloaded with details. To determine what is necessary for the scenario, the programme group (and steering group committee) can establish a "need/nice to have" list.[121] A "need" is an element that must be part of the scenario, while a "like" indicates desirable elements to be included in the scenario.

The structure and content of the scenario laid out in a "master event list" consists of events, actions and injects.[122] The scenario can include both technical/operational and strategic dilemmas. Injects can be prepared for both levels, as would happen in a practical situation.

[120] *ISO 22398:2013(E), art. 5.3.4.2, p. 20.*
[121] *ISO 22398:2013(E), annex B, p. 27.*
[122] *ISO 22398:2013(E), art. 5.2.14, p. 17.*

Terms

Master event list – A timeline in which injects 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 goals of the exercise. A scenario requires different realistic events.[123]
Action – The consequences resulting from an event. An action is intended to provoke a response from participants. Participants must take action and make decisions based on the events. Reactions by participants move the scenario forward.
Inject – These are used to bring actions to participants' attention. Injects include social media messages (such as Twitter), newspapers and media messages, phone calls from stakeholders, phone calls from journalists and email messages from simulated contacts.

Technical preparation

To make the scenario realistic, you can use various tools and evidence such as websites and (fabricated) leaked documents. All sorts of technical game elements can be added to practise the technical side. Examples include malware, the application of Raspberry Pi in the network and simulation environments of existing production environments. Technical resources of this kind need to be prepared and created in advance.

Briefing for participants

It is recommended to inform all participants prior to the exercise of the rules and mutual expectations. This can be in the form of an information pack with a personal briefing explaining the exercise, rules, address book and background information. Participants will know what to expect and what is expected of them, and will feel involved as a result. This ensures that the simulation runs smoothly. A lead-in or teasers can be distributed to introduce the scenario. This ensures that all participants start with the same information and are ready for the exercise.

4.2 Execution

Roles during the exercise

- The **exercise leader** supervises the central scenario, consults with the response cells in order to identify how the exercise is progressing, and offers guidance when necessary. They can add or remove injects and offer alternatives to make the exercise as realistic as possible.
- The **central response cell** simulates all roles from the outside world, such as municipalities or other public authorities, emergency services such as police and fire departments, associations, journalists etc.
- The **internal response cell** distributes the injects throughout the organisation and simulates all the roles of the internal stakeholders who are not participating in the exercise.
- An **observer** can be designated for the duration of the exercise. Observers can see in the workplace whether and (if so) how the goals are being achieved. Such observations can contribute to the evaluation process.[124] The observer can also communicate with the internal response cell to adjust the scenario using injects.
- **Participants** are the players who are faced with the actions and injects in the field. They take action and make decisions to manage the crisis scenario as if they are actually dealing with a crisis.

[123] *ISO 22398:2013(E), art. 5.2.14, p. 18.*
[124] *ISO 22398:2013(E), art. 5.4.2, p. 20.*

Role of the participants

During the simulation exercise participants must respond as they would do during a normal working day. That means they start at the same time or work from home as usual, and make contact as they normally would. This makes the situation as realistic as possible. If they want to get in touch with someone who is not participating in the exercise, they must contact the response cell.

Start-up briefing

It is recommended to have a short start-up briefing with the response cells before the exercise starts. This is an opportunity to discuss the goals and the collective use of premises, telephones and the address book. The rules for the role-play are also discussed and the attendees briefly run through the scenario and set out the conditions for a possible suspension of the exercise.[125]

Execution of the exercise

The distribution of the first injects sets the scenario in motion and provokes the first actions. The response cells then provide injects to keep the exercise going. The participants respond accordingly. This generates interaction between the participants and the scenario. The pressure on the participants will grow as the exercise develops. This prompts many actions, decisions and a great deal of communication.

Injects may require both technical and strategic actions and decisions. An inject that displays a login error 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, both levels will actively seek each other out to communicate about the crisis.

At the end of the exercise, it will be scaled down and terminated. Unexpected situations may occur during an exercise, for example if a participant thinks it is a real crisis or emergency. In such situations, the exercise leader and response cells must be flexible and able to improvise. The exercise leader can stop the exercise temporarily or permanently.

4.3 Evaluation

An evaluation is *"the systematic process that compares the results of the measurement with recognised criteria to determine the differences between the intended and actual performance."*[126] The exercise is usually evaluated against the exercise goals. The exercise goals are therefore decisive for the evaluation criteria.[127] Structured monitoring and evaluation can help to apply the feedback and lessons learned within the organisation. [128] [129] The experiences of members of the project team, programme group and observers are used in the evaluation.[130] A survey can be used to obtain the opinions of the project team, programme group and participants regarding the project.

[125] *ISO 22398:2013(E), art. 5.3.2, p. 19.*
[126] *ISO 22398:2013(E)*
[127] *Evaluation criteria is decisive for ensuring the value of the crisis exercise.*
[128] *ENISA "On national and International Cyber Exercises" (2012), p. 18.*
[129] *ISO 22398:2013(E), p. 21.*
[130] *ISO 22398:2013(E), p. 22.*

Evaluating the exercise

The exercise can be evaluated at different levels. Firstly, the aspects that were successful can be assessed. In this case, the focus is on how the exercise is organised and how it is perceived by the preparation team and participants.

Examples of questions:
- How did the preparation phase go?
- How intense was the exercise?
- Was the scenario successful? Were there enough injects or too few?
- Did the scenario have the desired impact?
- Did participants find the scenario realistic?
- Did certain situations have an impact on the execution of the exercise?
- Are there any recommendations for the next exercise?

Evaluation of internal crisis processes

As well as assessing the execution of the exercise, it is possible to evaluate how the 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 into whether the crisis structure works as intended. Attention is given primarily to the correct course of action. The results can also be looked at. The results produced by the exercise process are highlighted in particular. This mainly concerns the efficiency and effectiveness of the measures taken.[131]

During the evaluation, questions such as 'what happened' (describe), 'why did that happen?' (explain), 'what does that tell us?' (analysis and reflection) can be asked to find points for improvement in terms of crisis organisation.[132] Lessons can be learned about the execution of the exercise and the effectiveness of the crisis management, which form the basis for improving the internal crisis structure.

4.4 Conclusion

Regardless of whether exercise goals are met, the exercise is successful because lessons have been learned. An exercise fails if it is not well organised, e.g. if the exercise is not well prepared, the scenario does not reflect the player's experience, or the exercise has to be stopped urgently due to an emergency. The preparation of an exercise is successful when participants have taken action and made decisions based on the exercise scenario, and when participants have had a realistic and instructive experience.

[131] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013) p. 29.*
[132] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013) p. 24.*

5. OZON CYBER CRISIS EXERCISE

5.1 Introduction

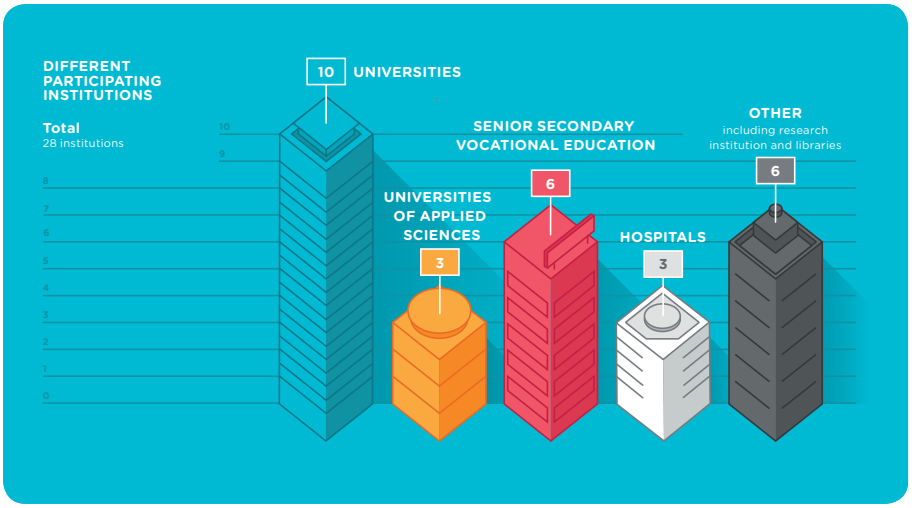
The cyber crisis exercise is emerging as a new tool for improving resilience against cyber crises. In 2015, SURFcert participated in the nationwide exercise ISIDOOR by the NCSC. Inspired by this, SURFcert, together with SURFnet, took the initiative to organise a cyber crisis exercise for education and research institutions. Organising a crisis exercise is a major task. SURFnet has deployed part of its innovation funds for a research programme into security and privacy.

Exercise

The exercise was carried out on 4 and 5 October 2016, from 8:15 am to 5:00 pm on the first day and from 9:00 am to midday on the second day. Planners and some of the players commenced an evaluation on the afternoon of the second day of the exercise. To be able to evaluate the intensity, duration, and any eventualities, it was decided to conduct the exercise during office hours.

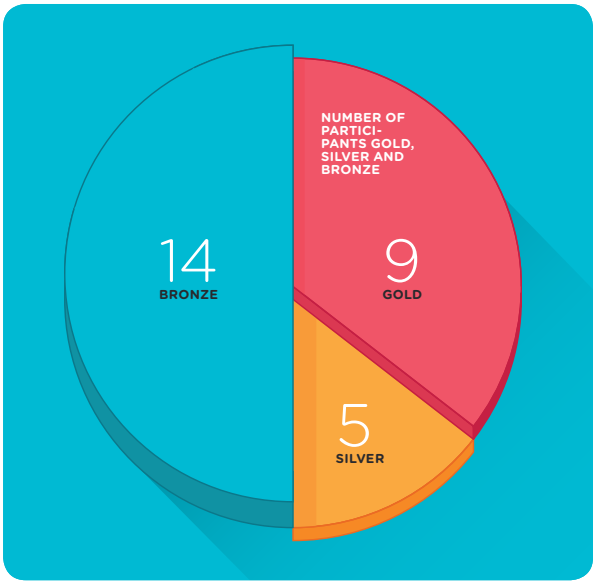
Participants

The 28 participants of the OZON Cyber Crisis Exercise hailed from the research and education sector, which included universities, colleges, schools, hospitals and research institutions. More than 200 participants were involved at the tactical, operational, technical and strategic level. Participants included security and privacy officers, ICT managers, members of Boards of Directors, staff services, incident response teams and communication and press officers. Institutions were able to participate at the gold, silver or bronze level. Registration had to be closed early due to interest beyond all expectations.



Level	Content
Gold	The Gold level developed a simulation scenario and practised building bridges between the tactical/operational, technical and strategic levels. Members of the Executive Board/Board of Directors participated.
Silver	The Silver level developed a simulation scenario and facilitated testing and training at the tactical/operational and technical levels.
Bronze	Bronze-level institutions observed the development of the simulation exercise. This provides knowledge and insight into the development and tackling of a crisis. Bronze level participants also received a "capture the flag" order.

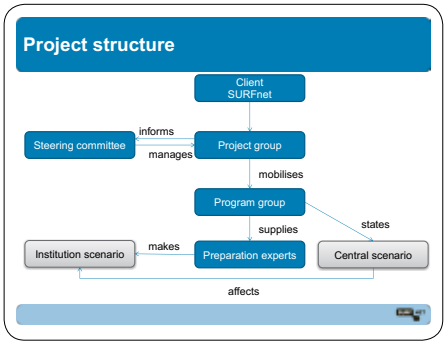
The exercise was initially started with 31 institutions as participants. The preparation of the crisis exercise was intense and should not be underestimated. Therefore, three institutions cancelled their participation in this phase, including one gold and two silver players. One institution chose to play at the bronze level instead of gold.



5.2 Prior to the OZON Cyber Crisis Exercise

Roles

SURFnet was **the client** for the OZON cyber crisis exercise. **The steering committee** consisted of eight gold players and made decisions at a strategic level.



The programme group consisted of the exercise preparation experts from the gold and silver institutions. The members of this group assessed the central scenario and devised and planned the institutions' scenarios. They briefed the institution's internal players to prepare them for the exercise. During the game, they acted as an internal response cell to keep the game going with necessary interventions.

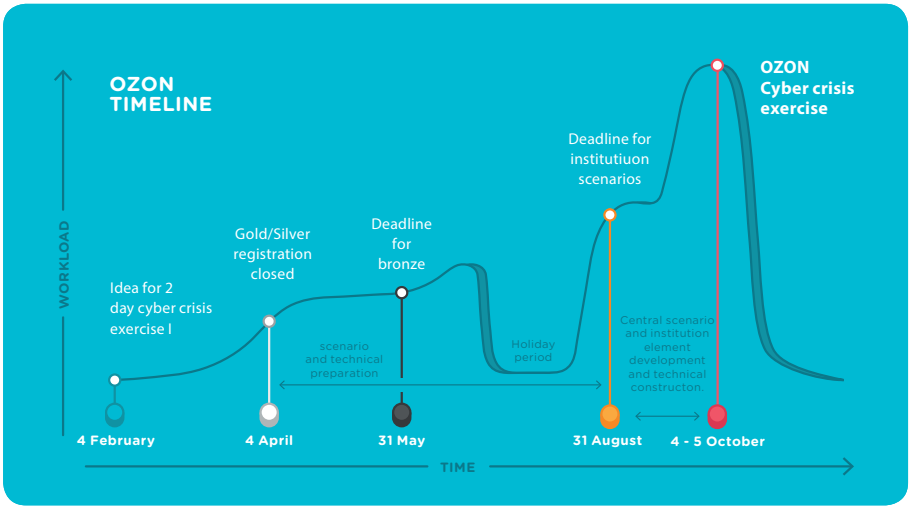
The project team took on the tasks of the umbrella organisation. The project team was comprised of a project manager, project secretary, communications officer, institution scenario supervisor, a couple of SURFcert members and a number of project members. The project team prepared the central scenario, helped the institutions to create and adjust their institution scenario and prepare and supply documents. This team was also the central intermediary for communication about the exercise.

The project team, together with the programme group, prepared the exercise both strategically and technically. Websites were built, simulation malware was written and Raspberry Pi units were configured and put in the field. The project team was also part of the central response cell.

External party – Because there was no experience of setting up such a large-scale cyber crisis exercise, external expertise was enlisted. Their role was to assist in the strategic execution, supply training resources such as the master event list and the media simulator, and provide support to the exercise leader.

Schedule

The entire preparation process from idea to execution took eight months. The eight-month period started with the development of the idea and budgets, the accumulation of support within SURFnet, and the creation of a project group. Invitations were then sent to the members of SURFnet (Research and education institutions). Registrations had to be closed before the deadline due to the quantity of interest. The project team, steering committee and programme group wrote the outline of the scenario and drew up a "need/nice to have" list. In the following months, the institution scenarios were technically and strategically prepared in coordination with the programme group. This took up the majority of the preparation time. After the institution scenarios were completed, the scenarios were worked out in detail, newspaper articles were written, and tweets were prepared and recorded in the media simulator. The steering committee met a total of three times, and the programme group met a total of five times.



Internal communication

For internal communication during the planning phase, material, technical details, master event lists and communication about the exercise were shared via email and a wiki.

Briefing for participants

Participants were briefed prior to the exercise, and received an information pack, the rules and the address book for the exercise. To prepare participants for the exercise,

materials based on the context of the planned crisis scenario were shared. One of the participating institutions had a teaser video about possible attacks by the hacker group, and shared it with the other participating institutions.[133]

5.3 The exercise

Prior to the exercise, the primary and secondary objectives were established by the project group, steering committee and programme group. The institutions established their internal goals based on this.

Primary and secondary objectives

The central objective of the cyber crisis exercise was to increase the resilience and awareness of institutions in a cyber crisis. The secondary objectives were:

- Testing the chain reaction of such a cyber crisis event
- Testing the effectiveness of crisis communication
- Improving cooperation within and between institutions

Internal objectives

Institutions set internal targets based on the primary and secondary goals of the exercise. The most common internal objectives were:

- Promoting awareness about security.
- Increasing awareness about cyber crisis risks.
- Testing internal and external communication.
- Improving communication between operational and management levels.
- Testing whether internal process able to deal with a cyber crisis.
- Testing security protocols.

The scenario

Based on the predefined exercise objectives, the scenario was designed in which participants could practise both internal communication and escalation to the strategic level. A simulation exercise was therefore chosen in which players were faced with an exercise scenario in their own working environment. The exercise was both for crisis management and to provide IT departments with an important challenge. It was also important that the exercise contained enough recognisable and realistic elements for all the different institutions. The scenario had to contain enough complex dilemmas to determine whether participants could make decisions in time.

To ensure that the crisis could not be solved without turning to the strategic level, a scenario was written with both technical and strategic dilemmas that could not be solved without a strategic decision including all participants. Moreover, the central scenario featured an ethical element to ensure that institutions consulted with one another to deal with it.

With this starting point in mind, a list of dilemmas was established that required the Executive Board's attention:

- Reputation damage
- Claims
- Personal reputation
- Reputation of the organisation
- Administrative liability
- Ethical issues

[133] *See Chapter 4 for a description of the participants' briefing and the content of the information pack, address book and rules.*

These dilemmas could entail the following risks:

- Disclosure
  - Medical records
  - Personal data
  - Research data
  - Company data
  - Organisation data
- Extortion
- Encrypted data files
- Espionage
- Custom/manipulated data

Central scenario

The central scenario consisted of two simultaneous threats: an attack by an idealistic hacker group and a criminal element.

Given the above points, a fictitious idealistic hacker group that much of the Netherlands has sympathy for (including members of the institutions) was chosen for the exercise. This group has both an ethical and a criminal element. As a result, the dilemmas are not simply ignored. The threat posed by these hackers was aimed at the entire education and research sector. This promotes cooperation between institutions.

The hacker group considers that too much information is held by companies and authorities and is not being made public for economic reasons. Their view is that if all data was available to everyone, the development of human civilisation would be accelerated. Not sharing information hinders progress, which is why they are against all forms of intellectual property. Their goal is to make as much information fully public as possible. As a result, they do not take sensitive personal data into account.

The hacker group is highly regarded by the public with their declarations and announced that they are expanding their activities to the Netherlands, while focusing on the education and research sector. The scenario has a strong technical component for the hackers to achieve their goal. They have distributed malware on a wide scale. It is multifunctional malware that can collect and transmit files, but is also able to command the encryption of all the files on the computer or connected network. This means the hacker group can collect great quantities of sensitive data. The hacker group will make this data public in a media offensive.

Employees of the education and research institutions in the Netherlands are prompted to download the executable malware and install it on their institutions' computers. The executable file spreads via a Windows zero-day vulnerability and makes new data collection possible. A request is also made to create a mirror of the website containing disclosed data. Raspberry Pi units are used to simulate these mirrors.

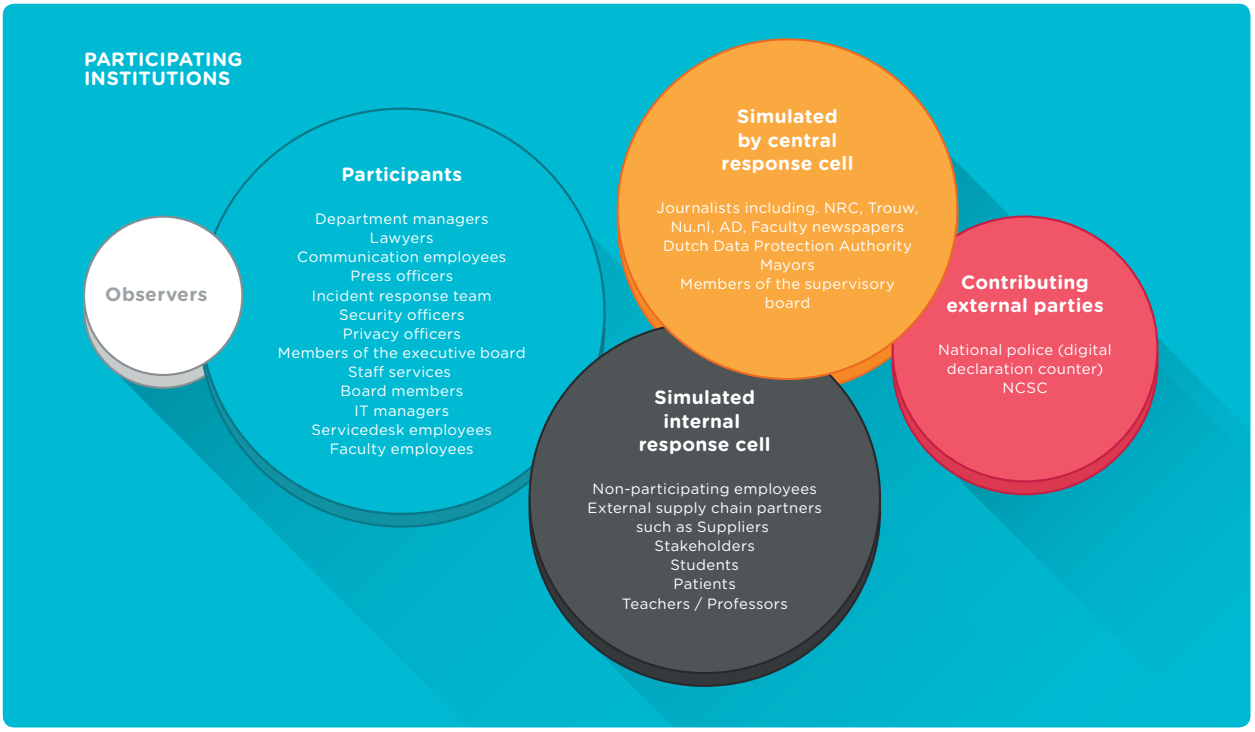
A number of professors initially expressed support for revealing the data. Although they condemn hacking, they are in favour of the revelations because of the ethical questions raised. A web petition to collect researchers' signatures is also started.

The scenario also has a criminal component. A journalist discovers a web portal where it is possible to adjust fees, disclose administration figures, disclose medical records of famous Dutch authority figures, reveal compromising photos of fellow students and teachers, and review exam data. A possible link to the hacker group is suggested, but it is not clear whether it is real.

Institution-specific scenario

The central scenario has an impact on the entire education and research sector. Based on the central scenario, institutions tailored their own institution scenario to their own exercise goals, participants and practice situation. In the preparation phase, a "need/nice to have" list was established as a basis for the institution's scenario. Because of the project team's unfamiliarity with the subject matter, institutions were actively supported to adjust their scenarios. This was to ensure that they were compatible with the main scenario and sufficiently challenging to involve technical, tactical and administrative participants in the exercise. Any information sensitive to public disclosure and systems containing this information in the institution were considered.

Once the sensitive information was identified, exercise planners had support from the project team to make the elements of the scenario as realistic as possible. [134] The exercise planners set out the final version of the institution's scenario in a master event list, i.e. a combination of events for the generic scenario and institution-specific events.



Role of the media and society

A special role was played by the media and society. The central response cell simulated the role of the outside world, as did various journalists, Boards of Trustees and the Personal Data Authority. Newspapers and social media reports were prepared in advance and were spread through a simulated environment during the exercise. During the exercise, the response cell simulated several phone calls from the press, regulators and other stakeholders. The national police participated with a digital declaration counter. The NCSC sent warnings to participants. The internal response cell simulated non-participating employees, external partners such as suppliers, and stakeholders such as students, patients and teachers or professors. The central and internal response cells orchestrated the exercise from a central location in Utrecht.

[134] *Injects included tweets, Facebook posts, newspaper articles, emails from stakeholders, and calls from stakeholders and journalists. Other communication media was also used, such as Jabber, WhatsApp and Skype.*

Closed environment

To monitor the closed nature of the exercise, an address book and separate SCIRT and SCIPR mailing lists were used.[135] The central exercise leader was accessible via a centralised email address.

Prerequisites for the success of the exercise

- **Impact on operational processes:** In order to avoid interruptions to daily operations, the exercise should have a minimal impact on operational processes.

- **Impact on infrastructure:** To avoid affecting the existing infrastructure, some institutions constructed a simulated environment. The institution could decide whether it wanted to use the simulation malware and Raspberry Pi units or not.

- **Role of security officers:** Because many security officers were part of the preparation team, they did not play their usual role in the exercise. Institutions found suitable solutions themselves. This was also an opportunity to see how the organisation functions in the absence of the security officer.

- **No-play situation:** The project leader had the power to stop the exercise (no-play situation). The no-play situation was not used during the OZON cyber crisis exercise.[136]

Exercise leader

Central exercise leadership is necessary for an exercise of this magnitude. For the OZON exercise, this role was played by the project manager and exercise leader (an external consultant for OZON). The exercise leader kept an eye on the development of the scenario and communicated with the response cells to discuss the progress of the scenario. For this reason, a short briefing was held every hour, at which the response cell briefly reported how the institution was reacting to the scenario. Adjustments were made by adding or reducing injects.

Observers

Most institutions had appointed an observer to watch over the internal crisis processes and meetings. These observations are useful for evaluating internal exercise objectives. Observers also communicated with the response cell on the progress of the scenario. This allowed them to make adjustments based on internal perceptions.

[135] *SCIRT and SCIPR are the security and privacy communities of the institutions affiliated with SURF.*
[136] *For an explanation of the no-play situation and other rules, see chapter 4.*

Exercise results seen from the response cell

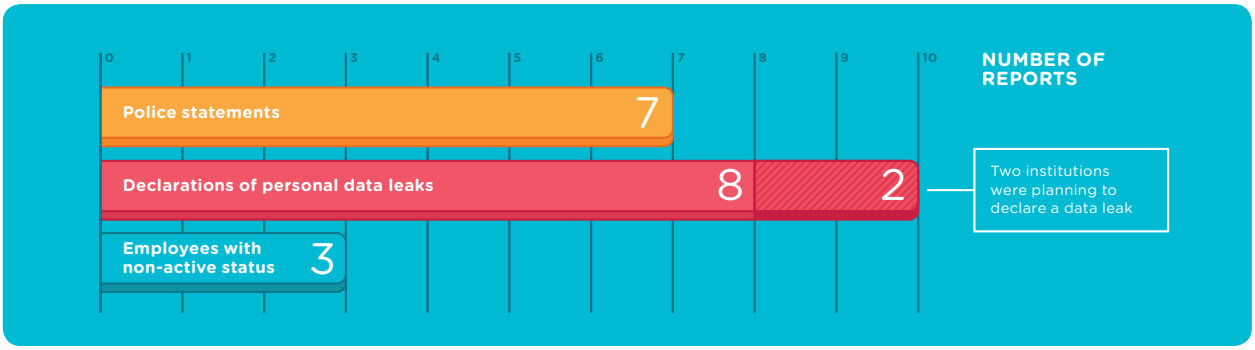
The start was initially hesitant. It was particularly exciting to see how the participants would react to the exercise. It quickly became clear that the reaction to the scenario was positive within the institutions. The institutions participated actively. The media simulator was monitored and institutions tweeted actively in the media simulator. The response cell could see that participants were actively involved and took their roles seriously. The exercise was highly realistic. The organisation was successful.

At first, it was believed that it might be necessary to add elements to the exercise to keep it going. By 11 am, however, it was apparent that the activity needed to be curbed rather than fed. Ultimately, adjustments were marginal. The injects found their way to the participants and they responded to them actively. The activity was constant and widespread during the day. The general atmosphere was positive.
Some simulations were brought to an end earlier than planned due to fatigue, and because for many institutions, their objectives had been achieved by the end of the first day. The freeze (finishing the game with a final signal) was somewhat unexpected. It turned out that some institutions were so engrossed in the exercise that they were still discussing possible consequences and strategies hours later.

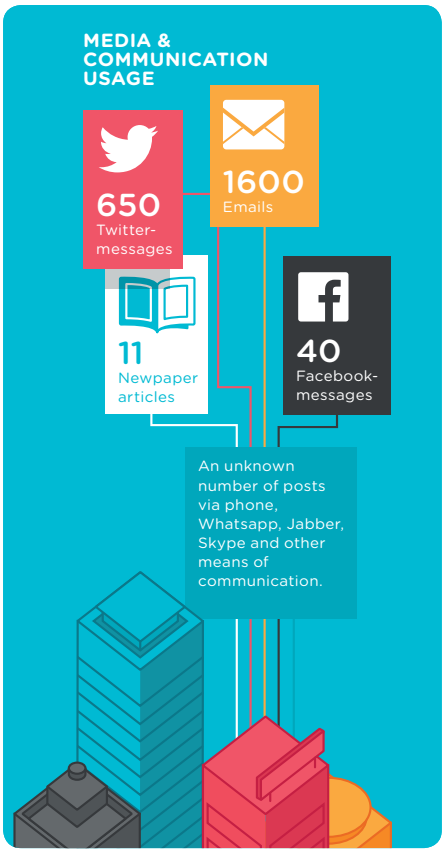
Players participated enthusiastically. Even board members who only joined on the first day for a few hours asked if they could play again. The second day was mainly spent extending the game of the first day. For some, a few extra injects were added. The game also proved easy to kick off on day two. It is worth winding the exercise down with targeted injects to give participants enough time to draw their efforts to a close.

There were no unexpected events that led to the shutdown of the exercise. One department within an institution withdrew because of too much pressure with their normal work load.[137] The exercise had no impact on the existing infrastructure. It was evident that the exercise was much more intense than foreseen. This point is discussed later with the results.

In total, the gold and silver players sent seven statements to the police and eight declarations to the personal data authority. Two bronze players wanted to make a declaration to the personal data authority. Also, three fictive employees were made inactive during the game.



[137] *The institution's exercise leader detected this from the internal response cell. The impact on overall progress was limited.*



Media reports and communication during the exercise

In total, 650 tweets were sent during the one-and-a-half-day exercise (of which 500 were already prepared). A total of 40 Facebook posts and 11 newspaper articles were published. The institutions exchanged over 1,600 emails.[138] These email exchanges were logged in a central Cc-address.

Bronze participants

Bronze participants observed the simulation exercise. They had access to the media reports which reflected the evolution of the crisis. They were also given a "capture the flag" exercise. A student provided with software on a laptop computer that could be detected in the network was located in or near the bronze participant's building. To optimise the surprise effect, bronze participants were not informed. In practice, however, it became evident that most bronze participants only expected a simulation. Even after several emails were sent from SURFcert, many institutions apparently did make a start internally, but did not actively try to find the student. The conclusion is that in a future "capture the flag" exercise, at least one or several employees should be informed so they can actively manage the exercise internally. This would enable this element of the game to show its full potential.

5.3 Evaluation

Evaluation contributes to the formulation of points for learning and improvement. Listing positive elements, meanwhile, helps to develop both the exercise and the internal crisis process. At the end of the second day, 45 participants and exercise preparation experts took part in the evaluation. Not all participants were invited to take part in the evaluation. This was partly due to lack of space. Prior to the central evaluation, an initial internal evaluation was conducted by the institutions. The results of internal evaluations are included in the central evaluation.

During the evaluation, generic elements were discussed in particular, such as the central exercise goals and the extent to which the exercise had met them. The evaluation did not examine how the institutions functioned during the exercise. The institutions are responsible for drawing their own internal conclusions. A survey was also distributed to all participants. The results are shown in the following section.

[138] *All user emails were monitored by forwarding the sent emails to a Cc-address.*

5.4 Results

The results are based on the outcome of the evaluation and observations during the exercise. Elements covered:
- aspects of the exercise itself;
- exercise preparation;
- the impact of the exercise;
- internal communication and coordination;
- information sharing between institutions;
- interpreting information;
- awareness and
- capture the flag (bronze exercise).

5.4.1 Exercise

- **Realistic scenario**
  The evaluation showed that the participants were satisfied with the scenario. Many players indicated that they considered the exercise to be both very realistic and instructive. The Steering Committee requested that the exercise be as realistic as possible. This was successful.

  The scenario contained sufficient strategic and technical challenges, and the level of the scenario reflected the exercise goals. All participants found the scenario engaging. Nothing important was left out of the crisis exercise. At no point did the scenario go awry, and there were no surprises during the execution. Any improvisation consisted mainly of re-enactments of parts of the scenario.

  The widespread nature of the exercise made it possible to include many players, including both institutions and external parties such as the police, the Dutch Data Protection Authority (DPA) and the NCSC. This made the exercise even more realistic. The steering committee was unaware of the exercise scenario, so members were able to play their own role. This was not perceived as a problem. It is even better to know nothing about the contents of the exercise. This enabled them to fulfil their own roles. Social media and newspapers reports were realistic additions. The messages were read and there was active concern in many institutions.

Lessons learned
- To distribute the media reports, it is advisable to use a searchable and intuitive simulation environment.
- The OZON Cyber Crisis Exercise successfully created a realistic exercise.
- A realistic scenario contributes to the participants' experience, creating a fiction that is perceived as very realistic and instructive.
- It is easier to include external parties in a large-scale exercise. These parties include organisations such as the DPA, the NCSC and other parties.

- **The relationship between the central scenario and institution scenarios**
  The central scenario created a cross-institutional cyber crisis. The institutions could use this base to build their own scenario. They found this to be a very valuable experience. Each institution could adapt the scenario to its own needs and exercise goals. The modular design was successful.
  During the preparation, the emphasis shifted from a centralised cyber crisis to a cyber crisis within the institution. A number of collaborative relationships were established from the beginning between different institutions such as regional

training centres and hospitals. This made it possible to create a common scenario and reduce the burden of preparation. But unfortunately these shared scenarios did not live up to expectations. This is partly due to a lack of knowledge about the cyber crisis exercise and partly because pressure was put on internal processes. This led to many different "inwardly focused" institution scenarios. Given the current organisation, the number of participating institutions was ideal.

Lessons learned
- The overall scenario was complicated because a specific scenario for each institution was created in parallel with the central scenario.
- Given the current design of the exercise, the number of participants was optimal. More participants would have confused the exercise.
- Having the possibility to adapt the central scenario to the needs of each institution was considered to be very valuable.
- The modular design was successful.

- **Management involvement**
  Many institutions had high management level participation. In one institution, for example, management was scheduled to play for two hours. Because they found the exercise to be highly realistic and instructive, they made room in their schedules to participate for longer than was planned. Enthusiasm to participate was very high, resulting in the premature closing of registration for Gold members (management level).

Lesson learned
- The OZON cyber crisis exercise has put cyber threats on the agenda for management.

- **Participation of the players**
  The enthusiasm of the participants for the exercise was striking. Most players were seriously involved. For example, at the end of the first day, participants continued to discuss the plan and continued playing well after the signal was issued to stop the game. The participants worked hard and were concentrated.

Lesson learned
- Having a realistic setting and a specific scenario enabled participants to practise as realistically as they would in a genuine crisis.

5.4.2 Preparing the exercise

Preparation of the exercise took longer than expected for both the project team and the institutions. The evaluation shows that the preparation was justified. A great deal of time was invested in the development of the central and institution-specific scenarios. The holiday season was a particular obstacle for the planning. Smaller institutions had trouble mobilising sufficient resources to prepare an exercise on this large scale.

The need for both technical and strategic expertise to design a realistic scenario also came to light. This was a challenge for certain institutions. Once the right people with the right skills had been assigned to the team, preparation was able to get underway. The evaluation revealed a high level of confidence in the preparation team, which had demonstrated great enthusiasm and enormous commitment.

Lessons learned
- Development of the scenario at technical and strategic level required a lot of time and expertise.
- Setting up and organising a cyber crisis exercise was new to everyone involved. This is why preparing, developing and organising the scenario was considered to be complex.

- **Assistance in preparing the scenario**
  Support from the project team for setting up the institution scenario was highly valued. It was also helpful for getting production started. Concrete examples of dilemmas, the creation of a master event list and various game elements contributed to establishing a realistic scenario. Several members of the exercise preparation team emphasised this point.

Lesson learned
- Assistance with devising and setting up the institution scenario is highly valuable. Concrete examples of dilemmas, the creation of a master event list and various game elements contribute to the establishment of an institution scenario.

- **Support**
  Some preparation teams found it difficult to generate enthusiasm for the exercise among participants at their institution. After the exercise, participants indicated that its importance had become much more apparent. Institutions also took a long time to decide whether they wanted to participate, and at what level (gold, silver or bronze). It is important to take this into account when organising a crisis exercise. Furthermore, organising a large-scale exercise has a magnetic effect.

Lessons learned
- Sharing the results of exercises, communicating about exercises and practising on a small scale ensure support at the operational and strategic level.
- The preparation phase needs to take into account the time required for institutions to make decisions.
- Joint exercises create support within the sector.

5.4.3 Impact during exercise

- **Role of the internal response cell and the observer**
  Once the game was up and running, the pieces fell into place for the internal response cells. The internal response cells supervised the game closely and intervened when needed; they either operated on their own initiative or in consultation with the central response cell and exercise leader. The role of the internal response cell was performed successfully. However, members felt it

necessary to have a good overview of what was going on at the institution during the exercise. For this it was extremely valuable to have an observer on site. Furthermore, the response cell did not have the full picture of all communication within the institutions. Only part of the overall picture could be followed remotely. The observer role was also very useful for evaluating the internal processes.

Lessons learned

- It is relevant for the internal response cell to carefully monitor what is going on within the institution and to adjust if necessary in consultation with the exercise leader.
- The observer can share information with the internal response cell, but also has added value for the internal evaluation.

- **Closed environment**

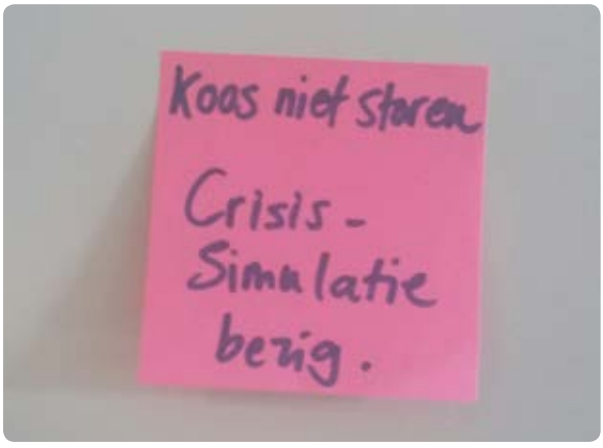
  The closed nature of the exercise was well preserved. There was only one case of non-participants becoming involved in the exercise. A participant was unable to distinguish between an exercise situation and reality in only one instance. The game elements were adjusted accordingly to avoid further confusion. In certain communication items, in this case emails, participants had to be reminded to use the exercise code.

Lessons learned

- The game rules, closed simulation environment for media reports, closed list of participants, and closed environments such as email and OZON-SCIRT and OZON-SCIPR contributed to securing the restricted nature of the exercise.

- **Intensity of the exercise**

  Participants found the workload of the exercise to be more intense than initially estimated by those who prepared the exercise. Given that it was the first exercise to be prepared and organised, the organizers had insufficient experience for estimating the workload. During the preparation phase, the organizers thought there would probably not be enough game elements. As a result, additional elements had been prepared to provide more content for the exercise if needed. However, they were not used, as the exercise proved to be sufficiently challenging. During the exercise, it was mainly the communication departments that were more heavily taxed than expected. This made it clear that communication plays a significant role during a major crisis.



Within two institutions several departments stopped participating prematurely because priority was given to internal business. The internal response cell took over the role of the withdrawn participants. Furthermore, some institutions decided to stop adding new interventions on the second day because exercise objectives had been met and further training was unnecessary. The rules created additional pressure, because participants were obliged to respect them and thus had to use the address book. This differs from the normal procedure in a crisis.

Lessons learned

- A realistic simulation exercise is very intense, especially if the scenario is as absorbing as the OZON cyber crisis exercise.
- A complex crisis requires much more time and attention from those concerned and cannot simply "be performed alongside normal tasks."
- The communications departments play a significant role in a major crisis.
- An exercise of this nature is effective due to its high intensity. This will be made clear from the outset for the next exercise.
- The exercise provided so many challenges and additional activity that the burden on institutions was greater than expected.

- **Loss of focus and stress on participants**
  At the end of the day, a decrease in participant focus was observed. The evaluation also showed this. This was due to both the pressure and intensity of the exercise, which was sometimes slightly too challenging. By regularly identifying and, where necessary, sending actions to institutions, it was possible to keep participants keen. Some institutions indicated that the pressure was only on certain participants. This may be due to the distribution of tasks within the crisis team. Personal commitment and/or stress during the exercise may also play a role.

Lessons learned

- Participants lose focus during a long and intensive exercise.
- Intervention in the form of increasing or reducing actions can contribute to maintaining participants' attention.
- The even distribution of tasks during a crisis makes for an even distribution of pressure on participants.
- Exercises help to clarify roles, responsibilities and their execution in crisis teams.
- It was evident during the exercise that some people were too invested. It is important to find a balance between too much and too little commitment from participants, both during an exercise and a real crisis.

- **Duration of the exercise**
  One day of exercise was sufficient for some institutions. Other institutions were fanatically involved in the game at the end of the first day, and used the second day to get the crisis under control. Some participants also expected new developments to arise during the night. This was not the case in this scenario. This proves the benefit of clear communication regarding the framework of the exercise. It was also argued that more time between the exercise and evaluation would provide the possibility to draw more internal conclusions.

Lessons learned

- It is possible to test the entire crisis process in a one-day exercise on the condition that everyone can participate.
- Clear communication about the start, end and framework of the exercise ensures that participants have clear expectations.
- More time between the exercise and the central evaluation would make it possible to conduct an initial internal evaluation and present the findings as part of the central evaluation.

5.4.4 Internal communication and coordination

- **Escalation between roles and communication between different levels**
  Communication was effective at a technical and management level in many institutions. Most institutions were satisfied with the degree of internal escalation. They considered the cross-sectional involvement at all levels to be highly positive. In some institutions, it was the first time that a complete cyber crisis team at a cyber security level had been created. This was found to be highly instructive and useful. A clear division of roles allows for rapid escalation and ensures that the right people are involved. Familiarity with internal procedures also ensures that stakeholders can act quickly.
  Some institutions already had operational strategic crisis teams at the beginning of the exercise. This is not always realistic. It is also important to test the ability to form a crisis team and the response to the first signs of a crisis. During the game, it also became clear that some players needed other participants (not included in the participant list) in the game.

Lessons learned
- Management, communication and technology departments do not have much day-to-day contact. During the exercise, it was shown they can support each other in a crisis.
- Broad involvement at all levels was seen as very valuable.
- Although a simulation exercise does not reflect reality, it does provide insight into how employees would react in a real situation. Exercises help players to clearly understand the respective roles and tasks.
- There is a need for more intense communication within institutions.
- In some cases, other parties have a more important role to play than is initially foreseen.
- A gap-bridging exercise helps to build bridges between management, communication and technology. Exercises help to prepare for real crisis situations.

5.4.5 Sharing information between institutions

- **Use of existing communication tools**
  Generally speaking, existing means of communication such as SCIRT and SCIPR work well for sharing knowledge within the IT community. During the exercise, communication resources were not used optimally. Not all participants were familiar with the existing means of communication and communication lines. Furthermore, many key figures were in the preparation team, and therefore did not participate in the exercise. As a result, communication was not set in motion according to usual practice.

Lessons learned
- The absence of a significant number of key figures from the crisis exercise (due to their participation in the preparation phase) had an impact on the exchange of information during the exercise.
- SCIRT, SCIPR and other communication means and methods contribute to mutual cooperation.
- Not all institutions are featured on the SCIRT and SCIPR community lists. In a crisis, it is necessary to have a means to reach everyone, including non-members.

- **Key players were involved in organising the exercise.**
  Key players in organising OZON could not participate during the exercise. In a normal crisis, they would have been part of the crisis team. Some participants found this problematic, as they would normally have had a very active role in a crisis such as this. One of the exercise preparation experts played two roles, both in the preparation and during the exercise. In practice this proved to be very difficult. The conclusion was that it is preferable to choose and play one role.

Lessons learned

- It would be ideal if the security officers who were in the preparation team could also participate in the exercise.
- Playing a role in both the exercise preparation and organising the crisis is not recommended. It is better to choose one of the two roles and pursue that role fully.
- The absence of key players in the crisis organisation has an impact on the degree of knowledge and information shared between institutions.

- **Information sharing between institutions**
  It was clear both during the exercise and from the evaluation that the focus was more on the internal resolution of symptoms than on sharing information between institutions. This was particularly evident at the beginning of the exercise. Collaboration began at the technical level later in the game, but was not visible at an organisational level. There was some one-on-one contact, but not across the sector. Other communities such as press officers did seek out interaction. Furthermore, some educational and healthcare institutions joined forces to exchange information in order to cope with the threat.
  Once underway, contact between institutions was greatly appreciated. As a result, employees of different institutions who had never met before got to know each other. The desire was expressed to perform more exercises, both among themselves and across the sector.

Lessons learned

- The exercise established new contacts between institutions.
- More communication is needed between institutions and across the sector.
- A large-scale exercise with several institutions offers the opportunity to reinforce mutual cooperation, exchange knowledge and share expertise.

- **Coordination between the institutions**
  During the exercise, the institutions focused on their own crisis and only sought outside cooperation later on. This was true for both the technical and the strategic dilemmas. The evaluation showed that the reflex is to solve internal problems first, but cooperation proved to be more necessary. All of the institutions, for example, tried to solve the technical dilemmas themselves and did not inform other institutions about what they were doing. As a result, they were mainly concerned with suppressing the symptoms.[139] It is not efficient to have all participants examining the same Raspberry Pi or analysing the same malware.
  These actions could be much more coordinated. Furthermore, the role of parties such as the VSNU, VH and the MBO council was mentioned during the exercise. The question arose as to what extent there can or should be central coordination in a national crisis. It should be clear whether there is a mandate for this and to

[139] *(Such as taking mirrors out of circulation, resetting passwords, and analysing Raspberry Pi units)*

what extent, with respect of the mandate and autonomy of the institutions, and if actions can be coordinated centrally. Meetings pertaining to this issue between the relevant parties will be scheduled for further discussion.

Lessons learned
- Much attention was paid to suppressing the symptoms.
- More coordination and collaboration between institutions is needed.
- Establishing contacts is seen as very valuable.

5.5.6 Interpreting information

- **Overview and interpretation of information**
  Interpreting the situation is one of the most difficult tasks. During the exercise, it became clear that participants found it difficult to understand the overall scope of the crisis. Good information exchange is therefore crucial. Thorough collection of information at technical, tactical/operational and strategic levels is necessary. The correct information must be available in the right location. All irrelevant information must be filtered out. Furthermore, each party and each level requires different information.

  As well as interpreting the information, the participants found the variety of sources of information and communication difficult. Participants found it difficult to keep track of all the different media, such as media reports, calls from journalists, internal communication and various chat environments and emails. The quantity of information will only increase in the future. Methods are needed to process all of this information correctly.

Lessons learned
- Effective information sharing and thorough information collection at all three levels is necessary to obtain a complete and accurate picture of the crisis.
- A good structure for filtering relevant information, with the right people providing the right information, makes for a more efficient and faster system for processing pertinent information.
- The challenge is to present the entire situation and make decisive choices at both operational and strategic levels.

5.5.7 Awareness

Regular crisis exercises are conducted to practise dealing with physical and social risks. This is much less the case for cyber risks. The OZON Cyber Crisis Exercise has put the threat of cyber attacks and attention to cyber risks firmly on the map.

The evaluation shows that increased awareness among all participants was very positive. Institutions have increased actions to put cyber security on the agenda. It was also concluded that the awareness of many parties who have not yet participated needs to be increased.

Lessons learned

- The OZON Cyber Crisis Exercise has put the focus on cyber risks.
- Cyber crisis exercises contribute to raising awareness and developing skills at individual, organisational and collective levels.

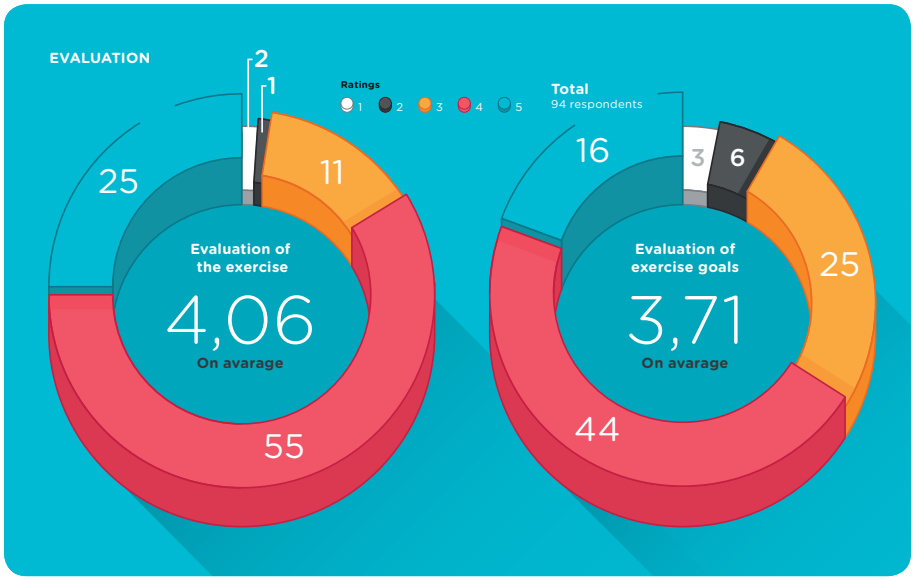
5.5.8 Capture the Flag (bronze exercise)

The bronze participants observed the exercise. As a result, most institutions had a good grasp of how a crisis can develop. They were also aware of a possible threat that could affect the institution. However, they were not previously informed of the presence of a student with simulation malware on their network. This was a conscious decision to test whether the institutions could detect and locate the students. As many bronze participants had been prepared for a simulation exercise, they were not expecting this. For certain institutions, the presence of the student was a surprise. The evaluation showed that this was mainly due to their expectations. Only a few institutions discovered the 'malicious' activity in their networks, they responded differently in solving the problem.

In retrospect, many institutions were positively surprised by the presence of the student. The institutions are planning on analysing the data. The exercise has provoked much discussion. Many institutions find the information useful. The capture-the-flag exercise contributed to the awareness and resilience of the institutions involved. This exercise goal was therefore met. During the exercise, it proved difficult to control multiple exercise systems simultaneously. Above all, the focus was on the students who were on site and getting the attack software work.

Lessons learned

- Observing the exercise has contributed to the awareness and perception of how a crisis can develop.
- The presence of the student in the network was not noticed due to of expectations given prior to the exercise. This led to a lot of conversation and analysis afterwards, with a positive effect.



5.6 Conclusion

The OZON Cyber Crisis Exercise is a successful first simulation exercise. The institutions and players participated actively and enthusiastically. The overall assessment of the exercise is 4.06 on a scale of 1 to 5 (average of 94 respondents, exercise preparation experts and players). The score was 3.71 for the evaluation of the exercise goals. Many institutions concluded that the exercise objectives were achieved at the end of the first day of play.

It was positive to see that there was a lot of communication between the different levels: management, communication and IT departments. Several managers asked if they could participate for a longer time. The players found the scenario highly realistic, fun and instructive. Some institutions also played fanatically after the closing signal and were still enthusiastic on the second day. The exercise is an extremely useful, very realistic and instructive experience.

The functioning of the system and the effectiveness of crisis communication have been assessed. The exercise shows that the division of tasks, internal and external communication and interpretation of information are a challenge. More coordination and direction both within the institution and between the institutions can contribute to faster and more efficient information exchange. This can also help institutions to seek solutions together at both tactical/operational and strategic levels. Establishing scenarios can help put more focus on cyber security risks.

The preparation phase was intense and took a lot of time for those preparing the exercise. The exercise also proved to be much more taxing for the participants than expected. It was difficult to foresee how escalation and communication between operational, IT and strategic levels would occur. Many efforts were made to make this effective in this scenario. A number of key figures were part of the preparation team; they were absent during the execution of the exercise itself. This was noticeable during the exercise.

The OZON Cyber Security Exercise is a gap-bridging exercise designed to build bridges between management and communication and IT departments both internally and between the institutions. Cooperation between and within institutions was also improved. The importance of the exercise for increasing awareness is tangible. This is a direct reason for devoting more time and thought to cyber security among institutions. Participants and exercise preparation experts learned much and gained a great deal of knowledge. Many stakeholders have expressed a wish to preserve and share this knowledge, and they have asked several times to repeat this exercise in the future.

6. RECOMMENDATIONS

Five main recommendations have resulted from the exercise:

- Make cyber security an integral part of crisis management and set out clear decisions about processes, roles and tasks in a crisis plan. A correct, balanced division of tasks and coordination in the crisis team provides clarity and guidance for all participants.
- Exchange information between institutions, and do so early in the crisis process. Make more use of existing networking opportunities. This makes it easier for stakeholders to interpret information, coordinate the process and tackle shared problems.
- Conduct research into the appropriate form of national coordination in a cross-sector cyber threat. In addition, carefully define the autonomy of institutions and the mandate to carry out such actions.
- Hold large and small-scale exercises aimed at the sector or on a particular topic on a regular basis to raise awareness, support and resilience. [140] Work together because preparing and executing exercises takes a lot of time and effort.
- Present the findings, conclusions and recommendations of exercises to improve awareness for cyber threats and gain support for cyber exercises.

6.1 Recommendations for crisis situations

We make a distinction between recommendations for the crisis situation and for the exercise. We offer the following recommendations for effective internal crisis processes and cooperation between institutions:

Internal crisis processes

- Make cyber security an integral part of the crisis management system and use existing lines of escalation.
- Clearly define the process, roles and crisis team tasks in the crisis plan. A correct and balanced division of tasks and coordination within the crisis team can help to speed up information sharing and improve cooperation and support for all those involved. Dividing tasks in this way also contributes to a better distribution of pressure. Do not be too rigid and make maximum use of knowledge, creativity and the ability to improvise.
- If you suspect that a crisis is going to last longer than predicted, set in place several crisis teams that can rotate. Ensure timely escalation and transfer to ensure continuity and confidence.
- Exercise regularly with different team configurations, and practise both with and without key players.

Cooperation between institutions

- Use mutual networking capabilities such as SCIRT and SCIPR more in order to reinforce mutual contact. As a result, institutions will reach each other more promptly in a real crisis.
- Promote information sharing between institutions in the crisis process. This makes it easier for stakeholders to interpret information, coordinate the process and tackle common problems.
- Investigate the possibilities of national coordination in a cross-sector cyber threat. Central coordination for analysis and interpretation can be positive as long as the autonomy of institutions is guaranteed. Incident handling must be controlled locally. The mandate for this needs to be well defined.

[140] *For example, hospital, data leak, and digital manipulation variants.*

6.2 Recommendations for the exercise

We make the following recommendations for the preparation of the exercise, the execution of the exercise process and the choice of the type of exercise:

Preparing the exercise

- Adjust the length of the exercise according to the objectives. Check whether it is possible to limit the exercise to one day.
- Take into account the time required for decision making in institutions for the registration process.
- Give sufficient time and resources for the preparation of the scenario and exercise.
- Provide the preparation team with sufficient technical and strategic expertise by expanding the team or providing internal support.
- Take the opportunity to develop the preparation team's knowledge by organising joint work sessions and workshops. As a result, participants will be able to collaborate on the scenario, share experiences and broaden their knowledge. This will increase the level of cooperation during the exercise.
- It is time consuming to prepare elements such as messages. Set the deadline for establishing institution scenarios well before the exercise to ensure there is enough time.
- Use support from the project group and exercise preparation experts in designing the institutions' scenarios.
- Consider whether sharing working material is possible; this material includes master event lists and media reports. Examples are useful in the creation of a good, realistic scenario and promote cooperation.
- Manage the expectations of the participants in the run-up to the exercise so that they understand the constraints, and know what is expected of them and what to expect. A briefing, rules, and address book information contribute to this. Be aware of the workload that the exercise generates for participants.
- Take into account the role of key figures when organising an exercise. Consider who takes part in the preparation and who will participate in the exercise.
- Set aside more time between the exercise and the central evaluation so there is more time for an internal evaluation. The results of internal evaluations are useful for the central evaluation.

During the exercise

- Consider appointing an observer to monitor the internal processes. This helps to evaluate internal goals and provide feedback to the exercise management team, who can then monitor the progress of the exercise in the workplace.
- The central and internal response cells need to stay in close contact with one another. It is therefore recommended for them to operate in the same area. They should, at the very least, be able to communicate (e.g. by phone).
- Use a simulation system for media messages such as newspaper reports and social media. This adds transparency and preserves the closed nature of the exercise. Working with a closed address book also contributes to this.
- Communicate clearly during the exercise about the start, end and the limits of the exercise. Any announcements about changes to the scenario should be made in good time. This makes expectations clearer for participants.
- It is advisable not to combine conflicting tasks like the preparation and execution tasks together.
- Also consider appointing a person to prepare the exercise from the bronze-level institutions. This facilitates better preparation prior to the exercise, better management of expectations, and better execution of the exercise.

Specific exercises and scenarios

- Practise realistic cyber scenarios using different[141] types of exercises (see Chapter 3). Exercises increase awareness and give employees the opportunity to become familiar with procedures, roles and the division of tasks in the crisis team.[142]
- Develop scenarios that, for example, focus on universities, colleges, regional training centres, university medical centres and research institutions. Cross-sector scenarios also help to foster increased cooperation. This makes it possible to increase the scale of the exercise.
- A large-scale exercise like OZON has a major impact on organisation and preparation. Organise both large-scale simulation exercises and smaller exercises aimed at a specific sector, topic[143] or type of exercise.[144]
- Organise gap-bridging exercises on both large and small scales in order to promote communication and coordination between the different layers of management and the communication and IT departments.

[141] *Such as "tabletop", "capture the flag" and "red team/blue team" exercises: see Chapter 3.*
[142] *see Chapter 2 for a detailed description.*
[143] *For example, hospital, data leak and digital manipulation variants.*
[144] *For example, "tabletop" exercises for the strategic level and "capture the flag" for the operational level; See a complete overview in Chapter 3.*

REFERENCES

Norms and standards

- **SURF Juridisch Normenkader (Cloud)services 2016 -** consulted via https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html on 16 November 2016
- **Normenkader Informatiebeveiliging HO (2015)** (Moens, 2015) - consulted via https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html on 20 October 2016
- **Normenkader Informatiebeveiliging MBO (2015**) (Kennisnet/saMBO-ICT, 2015) consulted https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC2-Normenkader-Informatiebeveiliging-MBO-versie-1.0-Creative-Commons.pdf on 20 October 2016
- **ISO 27001:2013** ISO 27001:2013 Information security management, October 2013 consulted via http://www.iso.org/iso/home/standards/management-standards/iso27001.htm on 20 September 2016
- **ISO 22398:2013(E)** ISO 22398:2013(E) Social Security - Guidelines for exercises, September 2013 consulted via http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50294 on 20 September 2016
- **ISO 22301:2012** Business Continuïteits management, May 2012, consulted via http://www.iso.org/iso/catalogue_detail?csnumber=50038 on 19 september 2016

Sources

- **COT (2011)** Schaap, S.D, van der Veen, M.J., Hendriks van der Weem, C.J *"Leren van incidenten",* In vijf stappen beter voorbereid, COT, mei 2011 consulted via http://www.cot.nl/pdf/Leren_van_incidenten.pdf On 12 September 2016
- **COT (2014)** COT*, "Elf bouwstenen voor een crisisplan",* van incidentbestrijding naar crisismanagement, COT, maart 2014 Consulted via http://www.cot.nl/pdf/COT_Elf_bouwstenen_voor_een_crisisplan.pdf on 12 September 2016
- **COT (2016)** COT, *"Instituut voor veiligheids- en crisismanagement, bijlage bij het verslag van het vierde Regionaal kennisplatform Integraal Crisisplan Zorg: concept scenariokaart Cyberaanval",* May 2016 Consulted via http://www.otoportaal.nl/sites/default/files/redactie/icp_concept_scenariokaart_cybercrisis_regio_amsterdam.pdf on 15 September 2016
- **ENISA (2012)** Trimintzios, P., Razvan, G. *"On national and International Cyber Exercises",* Survey, Analysis and Recommendations "Cyber crisis Exercises Analysis Report", ENISA, 2012 consulted via https://www.enisa.europa.eu/publications/exercise-survey2012 on 12 September 2016
- **ENISA (2014) 01** Panagiotis Trimintzios, Roger Holfeldt, Mats Koraeus ea. *"Report on cyber crisis cooperation and management",* ENISA, November 2014 Consulted via https://www.enisa.europa.eu/publications/ccc-study on 05 September 2016
- **ENISA (2014) 02** ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats (27-01-2015 ed.). ENISA. Consulted via https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014 on 05 September 2016
- **ENISA (2015)** ENISA *"The 2015 Report on National and International Cyber Security Exercises"*, final, 0.99, ENISA, Dec. 2015 consulted via https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises on 12 September 2016

- **ENISA (2016)** De Muynck, Jo, Portesi, Silvia *"Strategies for Incident Response and Cyber Crisis Cooperation",* version 1.1, ENISA, August 2016 consulted via https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation on 12 September 2016
- **NCSC (2013)** NCSC, "*De aanhouder wint"* de wereld van Advanced Persistent Threat Factsheet FS-2013-02C, NCSC, Version 1.3, 03 October 2013 consulted via https://www.ncsc.nl/actueel/factsheets/factsheet-de-aanhouder-wint-advanced-persistent-threats.html on 10 September 2016
- **NCSC (2014)** NCSC, *Cyber security Assessment*, 2014 consulted via https://www.ncsc.nl/english/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat.html on 11 October 2016
- **NCSC (2015)** Cybersecuritybeeld Nederland 2015 CSBN, NCSC consulted via https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-5.html on 05 September 2016
- **NCSC (2016)** Cybersecuritybeeld Nederland 2016 CSBN, NCSC consulted via https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html on 20 September 2016
- **SANS (2012)** Janes, P. "*People, Process, and Technologies Impact on Information Data Loss*" SANS, November 2012 consulted via https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032 on 5 September 2016
- **SURF (2015)** SURFnet Cyberdreigingsbeeld Sector Hoger onderwijs en wetenschappelijk onderzoek, 2015 consulted via https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2015/cyberdreigingsbeeld-2015.pdf on 15 September 2016
- **Wein, Willems (2013) 01** Wein, B, Willems, R, *"Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie"*, Nijmegen, April 2013 consulted via https://www.wodc.nl/images/2062-verkorte-versie_tcm44-502151.pdf on 10 September 2016
- **Wein, Willems (2013) 02** Wein, B, Willems, R, "*Een raamwerk voor het effectief evalueren van crisisoefeningen,* Nijmegen, April 2013, consulted via https://www.wodc.nl/images/2062-volledige-tekst_tcm44-498999.pdf on 10 September 2016
- **Zannoni, Kuipers en Wensveen (2012**) Zannoni, Marco, Kuipers Frank & Wensveen, Maike, *'Realisme in veiligheid en crisismanagement'*, COT, May 2012, http://www.cot.nl/pdf/Realisme_in_veiligheids-encrisismgtMBOHO.pdf consulted on 15 September 2016
- **Zannoni (2016)** Zannoni, Marco, *'Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont',* April 2016 consulted via https://www.linkedin.com/pulse/voorbereid-zijn-op-een-cybercrisis-marco-zannoni?published=u on 05 September 2016

Websites

- http://www.bcmacademy.nl/nl/bcm-academy/informatie-over-het-vak/begrippenlijst Consulted on 10 October 2016
- http://www.cot.nl/pdf/COT-Leren-van-Dorifel-15-januari-2013.pdf consulted on 12 September 2016
- http://www.cot.nl/pdf/Artikel-COT-in-Magazine-Nationale-Veiligheid.pdf consulted on 12 September 2016
- http://www.cot.nl/crisismanagement/crisisoefeningen/walkthrough/ consulted on 05 September 2016
- http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ consulted on 05 September 2016
- http://crisismanagement.schoolenveiligheid.nl/algemeen/ consulted on 12 September 2016
- www.crisisplan.nl consulted on 12 September 2016

- https://www.cybersaveyourself.nl/ consulted on 10 October 2016
- https://www.encs.eu/wp-content/uploads/2015/08/2015_ENCS_Factsheet_Red-Blue_Training_v1.pdf consulted on 20 October 2016
- https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 consulted on 21-10-2016
- http://www.integraalveilig-ho.nl consulted on 10 October 2016
- http://www.integraalveilig-ho.nl/continuiteitmanagement/ consulted on 15 September 2016
- http://www.pm.be/oefeningen_op_maat/command_post_exercise.html consulted on 12 September 2016
- www.ncsc.nl consulted on 15 September 2016
- https://www.ncsc.nl/actueel/nieuwsberichten/internationale-oefening-cyber-europe-2012.html consulted on 15 September 2016
- https://www.ncsc.nl/actueel/nieuwsberichten/duits---nederlandse-oefening.html consulted on 20 October 2016
- https://www.nctv.nl/organisatie/cs/index.aspx consulted on 20 October 2016
- https://www.surf.nl/persberichten/2015/12/surf-publiceert-cyberdreigingsbeeld-2015.html consulted on 15 October 2016
- https://www.surf.nl/diensten-en-producten/cybersave-yourself/index.html consulted on 10 October 2016

Nieuwsbronnen

- http://www.nu.nl/algemeen/1565130/brand-verwoest-faculteitsgebouw-bouwkunde-in-delft-video.html consulted on 20 October 2016
- http://www.nu.nl/tech/3627406/16-jarige-jongen-opgepakt-cyberaanval-school.html consulted on 16 October 2016
- http://www.at5.nl/artikelen/148428/waarschuwing_voor_phishingmail_inholland consulted on 20 October 2016
- http://www.rtvutrecht.nl/nieuws/1461998 consulted on 20 October 2016
- http://www.bbc.com/news/technology-36478650 consulted on 16 October 2016
- http://infosecuritymagazine.nl/2015/03/11/vrije-universiteit-amsterdam-besmet-met-ransomware/ consulted on 16 October 2016
- http://www.nu.nl/internet/4280591/studentgegevens-uva-en-hva-waren-makkelijk-vindbaar-systeemlek.html consulted on 16 October 2016
- http://www.nu.nl/internet/2427939/hackende-scholieren-betrapt-cijferfraude.html consulted on 16 October 2016
- http://www.nu.nl/binnenland/3931116/cijferfraude-leerlingen-amsterdams-gymnasium.html consulted on 16 October 2016
- http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html consulted on 16 October 2016
- https://www.nederlandict.nl/news/telecomsector-bouwt-met-grootschalige-oefening-cyberdawn-aan-sterke-samenwerking-op-cyber-security/ consulted on 20 October 2016
- http://webwereld.nl/security/79360-nederland-wint-goud--zilver-en-brons-op-wk-ethisch-hacken consulted on 21 October 2016

OZON TIMELINE

start · meeting · action · deadline · evaluation

WORKLOAD

TIME FOR

- 4 February — Idea for two day cyber crisis exercise
- 24 February — Kick-off meeting; Create budget and support; Forming project group
- 15 March — Invitations sent; Registration
- 4 April — Silver/gold registration closed
- 15 April — Initial gold registration deadline; Assamble steering committee
- 20 April — First steering committee meeting; Determine scope and objectives exercise
- 27 April — First steering committee meeting
- 28 April — Initial silver/bronze registration deadline; Establish central scenario in writing
- 12 May — Conclusion central scenario
- 18 May — Second programme group meeting
- 31 May — Bronze registration closed; Formulate institution scenario dilemmas and draw up master event list and game elements
- 8 June — Third programme group meeting
- 29 June — Second steering committee meeting
- 6 July — Forth programme group meeting
- 8 July — Holiday period
- 20 August — Deadline for institution scenarios
- 31 August — Draw up institution scenarios master event list and game elements
- 7 September — Last steering group meeting
- 15 September — Extension deadline institution scenarios
- 30 September — Technical elements ready (malware / logfiles / websites)
- 1 October — Briefing van deelnemers
- 3 October — Last programme group meeting; Raspberry Pi's distributed
- 4 / 5 October — Briefing response cell; OZON Cyber Crisis Exercise; Draw up central and institution elements, total master event list and complete media simulator
- 25 October — Evaluation OZON Cyber Crisis Exercise; Evaluation and formulation of outcomes of OZON Cyber Crisis Exercise; Evaluation and formulation of outcomes of OZON Cyber Crisis Exercise
- 1 November — Evaluation and formulation of outcomes of OZON Cyber Crisis Exercise

CREDITS

Text
SURFnet

Authors
Sandy Janssen, Alf Moens

Design
Vrije Stijl, Utrecht

Photos and illustrations
Alf Moens, Charlotte Verhees, iStock, Jaap van Ginkel,
Thomas Rohlfs, Studio Taeks, Amsterdam

November 2016

SURFnet

+31 (0)88 787 30 00
www.surf.nl