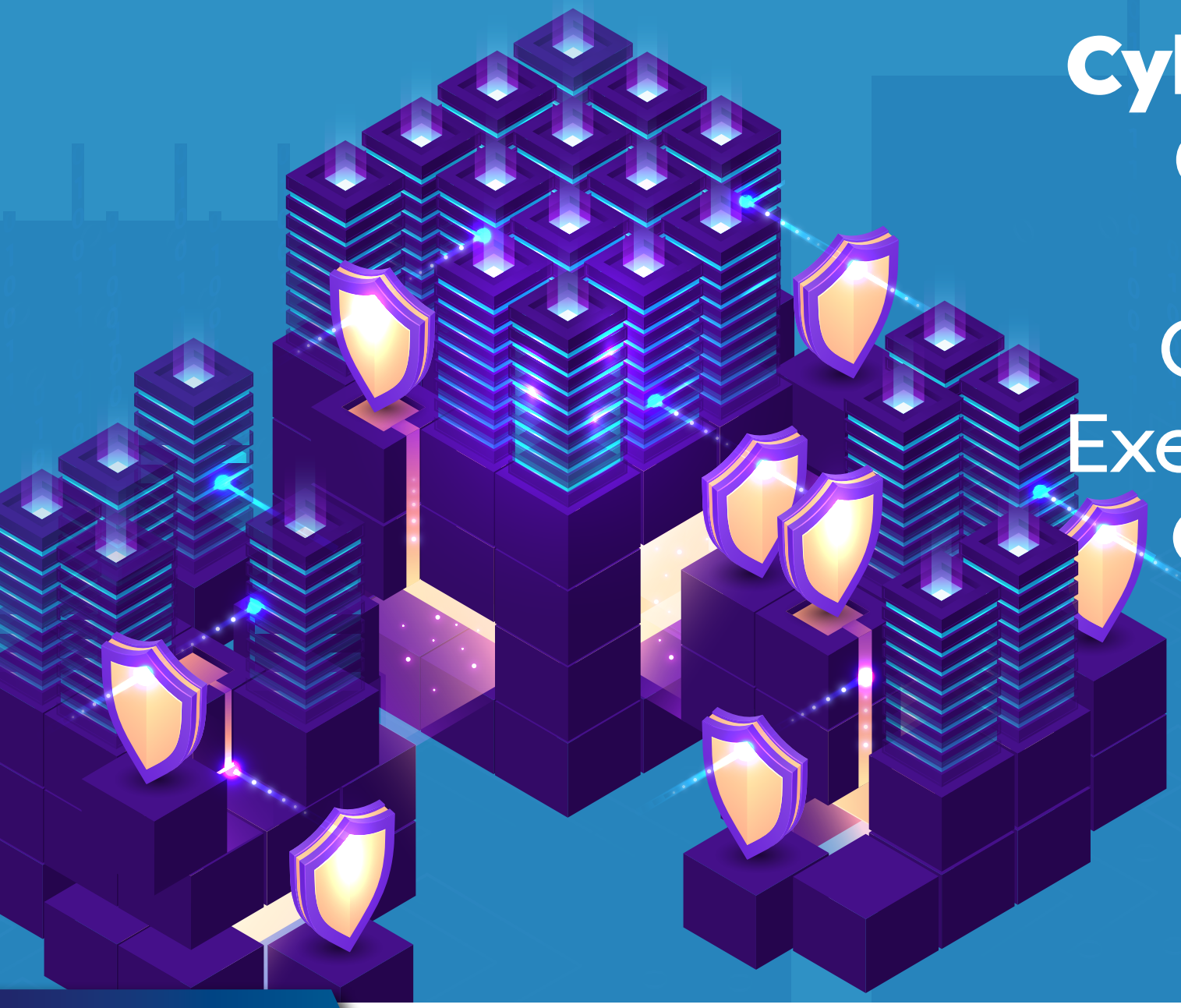


Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization

Cybersecurity Best Practices

A.09

Volume A:
A methodological approach

IDB

Cyber Israel
National Cyber Directorate

Originally published by the Israel National Cyber Directorate in Hebrew under the title *"Cyberpractice: Building and editing cyberexercises for the organization."* © (2020) Israel National Cyber Directorate.

This document was originally published by the Israel National Cyber Directorate (INCD) in Hebrew. Its translation into English was carried out by the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) division of the Inter-American Development Bank (IDB), and it is included as a chapter of the "Cybersecurity Best Practices" collection.

The reader should keep in mind that cybersecurity is a rapidly evolving field. Although these documents reflect established principles, they may be periodically updated as necessary to reflect developments in this field. Additionally, while every effort has been made to present the recommendations and resources in a way that is universally applicable to organizations around the world, the reader may find references that are specific to Israel's cyberecosystem and context (such as the amounts indicated in New Israeli Shekels [NIS], or references to Israeli law or government agencies).

The original document is available at: **https://www.gov.il/he/Departments/General/cyberexercise**. Please note that it includes the following disclaimer:

Contents

Foreword

Digital Transformation and the Challenges of Cybersecurity

As digital transformation continues to expand throughout the world, governments, organizations, individuals, and even objects are increasingly connected to the internet. Although digitalization offers undeniable benefits, such as efficient public service delivery, economic growth, and essential connectivity, it also contributes to our growing collective exposure to cybersecurity risks. Recently, the global COVID-19 pandemic has been an important driver of this phenomenon. As a result of widespread social distancing policies, the number of e-commerce transactions and online personal communications grew sharply in a short period of time, along with the number of employees who began teleworking for the first time. In this unprecedented situation, many internet users undertook novel online interactions without enough awareness of the security risks involved. Organizations had to quickly adapt to these challenges by setting up fully remote workflows, often without all of the necessary security measures in place or appropriate guidance to employees.

Cybercriminals are quick to exploit the uncertainty and vulnerability of unsuspecting individuals. Phishing and other social engineering scams proliferated, taking advantage of the global need for information related to the pandemic and the massive use of videoconference applications. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in only a week. Hackers posing as the World Health Organization sent phishing emails and massively spread malicious links to fake videoconference meetings and attachments containing malware. According to the Check Point Research 2021 Security Report, in the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. In the second half of the year, as more organizations strengthened the security of their remote platforms, hackers focused their efforts on exploiting vulnerabilities in employees' private assets and remote access devices to penetrate their organizations. Although such threats were maximized by this global context, they are not novel and will not go away; we continue to live in an environment of heightened risk, which is particularly serious in regions of the world where cybersecurity policies and technology are less developed and where citizen education and awareness around this issue are lacking. In other words, although the shifts due to the COVID-19 pandemic may revert to what they were before the pandemic, they have brought to light the urgent need to strengthen individual and collective protections against cyberrisks.

Strengthening cybersecurity is essential to safeguard citizens' rights to privacy and property in the digital sphere, promote citizens' trust in digital technologies, and support economic growth through safe digital transformation. In particular, citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services that they need. Moreover, security breaches have a significant negative economic impact. A recent report by McAfee estimated that cybercrime costs the world economy around US$6 trillion annually, or 0.8 percent of global GDP.

Israel: A Global Leader in Cybersecurity

Israel's innovation and entrepreneurship ecosystem is globally recognized as one of the most vibrant in the world, earning it the name Startup Nation. According to the March 2021 OECD Science and Technology Indicators, Israel is the country that invests the highest percentage of its GDP (4.9 percent) in research and development (R&D). The country is host to more than 300 research and development and innovation (R&D&I) centers of multinational companies. Of these, dozens are dedicated to cybersecurity.

It is no surprise that 40 percent of all private investment in cybersecurity worldwide takes place in Israel, which also has one of the world's largest private ecosystems in this area, second only to that of the United States. According to 2021 data, in that year US$8.8 billion were invested in around 131 Israeli companies from this sector, and more than 40 were acquired for a total of US$3.5 billion. Israel has more than 500 cybersecurity startups, and by 2021, 33 percent of the world's "unicorns" were Israeli. Overall, Israel's export of cybersecurity products was estimated in 2020 at US$6.85 billion.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience. The INCD operates at the national level to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities. Its positioning as part of the Prime Minister's Office clearly demonstrates the centrality and importance of its responsibilities. Its goals include to prepare and enable the Israeli private sector and general public to protect themselves from cyberthreats by adopting cybersecure technologies, publishing best practices, training personnel, and raising awareness. Furthermore, it aims to establish and strengthen the cyberscience and -technology base by developing highly qualified human capital, supporting advanced academic research, engaging in deep technological R&D, and fostering the cyberindustry. The INCD strives to maintain a protected, safe, and open cyberspace for all of the State of Israel's population and businesses and to facilitate the country's growth and its scientific and industrial base.

The State of Cybersecurity in the Latin American and Caribbean Region

The Inter-American Development Bank (IDB) carries out periodic assessments to capture the evolving capacities of its member states to defend themselves against the growing threats in cyberspace. The 2020 Cybersecurity Report, "Risks, Progress, and the Way Forward in Latin America and the Caribbean," developed in partnership with the Organization of American States (OAS), showed that countries were at varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement.

While in 2016, the year of the report's first edition, 80 percent of the countries in the region did not have a national cybersecurity strategy in place, this number had only fallen to 60 percent by 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure, such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors, to cyberattacks. As revealed by the 2020 report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrisome findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63 percent of countries had security incident response teams in place, such as computer emergency response teams (CERTs) or cybersecurity incident response teams (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding underscored the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyberincidents. Moreover, the report examined the availability of educational and training opportunities in cybersecurity and found that fewer than half of the countries in the region offered formal education in cybersecurity, such as postgraduate, master's, or technical degrees. Needless to say, having sufficient trained professionals is essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks.

The Inter-American Development Bank's Support to Strengthen Cybersecurity Capacity in the Region

For the past few years, the IDB has actively supported the region in the development of cybersecurity capacity, the design and implementation of national-level cybersecurity policies, and the strengthening of cybersecurity capabilities in the sectors it helps develop. This support takes a number of forms. The IDB has provided financial assistance amounting to tens of millions of dollars to develop national cybersecurity capabilities through more than 15 public sector investment loan operations, as well as significant additional funding to ensure the cybersecurity of digital transformation investment projects.

It also provides technical guidance and conducts cybersecurity projects across the region through consultancies, assessments, and tailor-made cybersecurity-strengthening projects on topics that include critical infrastructure protection, cybercrime and forensic analysis, design and strengthening of CSIRTs and security operations centers (SOCs), and national and sectoral cybersecurity strategies. In addition, the IDB has made substantial efforts to provide opportunities for Latin American and Caribbean professionals to strengthen and update their skills in this field by regularly offering workshops and training opportunities. These have included two-week cybersecurity executive courses, offered jointly with the Hebrew University of Jerusalem, as well as tailor-made courses on critical infrastructure protection and others targeted for specific sectors. Finally, the IDB has produced several high-impact publications dealing with national and sectoral cybersecurity issues, and continues to update and add to this body of knowledge regularly.[1]

1. See the website of the Data and Digital Government Cluster (DDG) of the IDB's Innovation in Citizen Services (ICS) division: **https://www.iadb.org/en/reform-modernization-state/data-and-digital-government-cluster**.

The IDB and the INCD: Joining Forces

The challenges of cybersecurity, like those of the internet itself, are global. Thus, sharing the knowledge and tools to meet these challenges benefits everyone. In recognition of this reality, the INCD and the IDB have partnered to make Israel's expertise in this area accessible to LAC countries. This collaboration has supported the LAC region in the form of executive and technical trainings on advanced cybersecurity topics, cutting-edge conferences for LAC public officials and professionals in the field, and innovative technical assistance projects. This publication is a product of this collaboration. It consists of a series of cybersecurity methodological guides for organizations, developed by the INCD in light of its analysis of risks, attack methods, cyberincidents, and globally accepted standards. These guides have been translated into Spanish and English as a joint activity of both organizations. They are being made available in these languages with the aim of providing access to this body of knowledge to audiences throughout the LAC region and contributing to strengthening cyberresilience in the region.

The challenge of protecting the digital space will continue to grow, along with the need for proven expertise to confront it. The insights contained in these guides are a resource to promote much-needed professional training in cybersecurity in the LAC region. These guides will contribute to raise organizational standards, promote greater awareness and a culture of cybersecurity within organizations and among the general public, and inform decision makers, managers, and leaders in their cybersecurity initiatives. It is our hope that these guidelines will serve as a roadmap for professionals and leaders throughout the LAC region, working together to build a more secure and prosperous future.

Introduction

The principles and rules for planning, creating, and conducting any exercise do not depend on the professional field in which it is performed. In this respect, practice is a generic activity. However, while the principles and rules are generic, their application in any professional field is not, but is influenced by the field in question.

In this view, the term "cybersecurity exercise" has meaning, since practice in this field has characteristics that distinguish it from practice in any other field.

This guide provides a conceptual basis for handling the field of practice—both in general and in the field of cyber. Specifically, it introduces the principles and rules for planning, creating, and conducting a cybersecurity exercise and the process of learning lessons from it. It also briefly discusses the construction of an annual and multi-year exercise program. Its subject of reference is the single organization, and the broader context of its content is the overall effort of the organization to maintain, preserve, and promote its cyberresilience.

Accordingly, the guide is divided into two sections: The first contains the conceptual basis. The second focuses on selected issues from the main part of the guide and provides guidelines for translating the conceptual discussion into practice.

There are four appendices on the following subjects:

01
Creating a cybersecurity exercise outline.

02
Creating a cybersecurity exercise scenario.

03
Conducting cybersecurity tabletop exercise and a cybersecurity organizational game.

04
Conducting a cybersecurity operational exercise.

As in other professional fields, the expertise required to create and conduct cybersecurity exercises can only be acquired through constant practice. This guide provides the reader with the theoretical basis necessary for practice in the field.

/01. Fundamentals of Practice

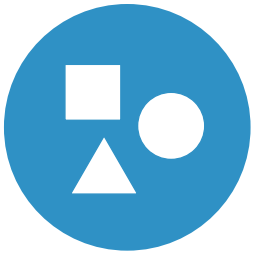
Basic Concepts

Exercise is a type of activity designed to perform, preserve, and promote organizational resilience. To understand its purpose, one must first know and understand the terminology. Two of the main concepts are competence and readiness.

Competence is the ability of an individual or of an organizational framework to exercise a particular function. **Readiness** is the ability of an organizational framework to perform a specific and concrete task. For example, in order for an incident response (IR) team to perform any of its regular tasks, each of its members should be able to perform the functions required of them to fulfill their role.

Competence expresses a generic, fundamental ability. Following the example above, it is possible that a certain competence of an IR team member meets the needs of some of the team's fixed tasks, and may even be required for fulfilling fixed tasks for other frameworks in the organization. In contrast, readiness expresses an ability directed toward a particular need or goal, and in many cases is suited to a particular scenario or environment of action. Moreover, it is always a feature of entire frameworks and organizations, not of individuals.

Readiness rests entirely on competencies. However, it is not only the competencies of individuals or teams, but also of means and resources (that is, the means being intact and the availability of resources at required inventory levels).



Competence and readiness of an individual and an organization are qualities that require gradual construction, ongoing maintenance, and promotion as needed and according to a plan. The overall responsibility for carrying them out rests with the management of the organization. The two main tools used by the organization for this purpose are **Training** and **Refresher**.[2] Training imparts and builds abilities, and a refresher preserves them. Thus, the main product of these two is an improvement in the ability of the individual or organization to function and fulfill their tasks. Training and refreshers are exercised, in practice, through courses, advanced training, and seminars.

Like any other activity, the organization's training and refresher activity requires supervision. Thanks to the fact that competence and readiness are quantitatively and qualitatively measurable, their level can be assessed using predefined and predetermined indices. The organization uses these indices to ensure that training and refresher courses are **effective** (i.e., that they achieve their goals), and that they do so **efficiently** (i.e., by making the best use of resources invested for this purpose). Operationally, this supervision is performed using two types of activities: **audit** and **exercise**.

Audit is a managerial activity, the main product of which is an up-to-date situation report of the audited body in the areas that have been chosen for inspection. By its very nature, auditing is an activity requiring judgment: the audited body is evaluated in a series of scores, determined according to the indices mentioned above.

2. There is a degree of ambiguity in conceptualization and terminology—both in Hebrew and English—in the field of instruction. In any case, in the military and security field it is customary to use the term "training" to denote any activity that involves learning or maintaining competency. In this view, therefore, training is the main tool for building competence and readiness.

Therefore, auditing is clearly an essential tool in controlling the organization's training and refresher activities.

In contrast, **exercise** is a learning activity designed to produce insights and lessons whose adoption and application will improve the competency and readiness of the organization. Therefore, an exercise is not a judgmental tool; conducting it is entirely intended to assist the organization, and not to put it in any threatening situation. Moreover, although both audit and exercise are intended for organizational learning, an audited entity tends to perceive the outcomes of learning derived from an audit as a disturbing interference in its internal affairs, or even as a punishment of the authority conducting the audit. In contrast, an exercised entity learns through personal experience, which encourages it to identify with and adopt the outcomes of learning.[3] The characteristics of exercise, and certainly the essential difference between it and audit, are extremely important, and must not only be in front of the exercise planners' and conductors' eyes from the time the exercise is initiated until the last conclusion is drawn, but also must be well understood by trainees throughout the process.

Below is a series of distinctions between the possible ways to practice, followed by a detailed discussion of the manner in which they will be used. Any exercise is based on simulating situations and circumstances that may occur in reality.[4] "Performing an exercise" means exposing trainees to the details of this simulation in a supervised manner and managing their response according to didactic principles and rules.

3. As part of an audit, it is customary to conduct an activity that is commonly called a "surprise exercise." Based on the above, it will be understood that this is not an exercise at all, but a kind of practical test based on simulation.
4. By their nature, exercises tend to rely heavily on simulation. One of the main reasons for this is the necessity to avoid causing damage as a result of using real components from the trainee's operating environment. **In the cyberdimension, this matter is particularly sensitive.** A detailed discussion of simulation in the exercise will be presented later in the guide.

Practice Methods

There are two methods for practicing: **theoretical** and **practical**.

In the theoretical method, trainees are required to deal mentally with challenges for which they have no ready-made response, often while demonstrating resourcefulness, creativity, and "out-of-the-box" thinking. The trainees' activities are based on discourse (discussions and team consultations). They do not actively respond to the events presented to them, but declare (usually orally, and sometimes in writing) what they would have done if it had been a real event.

Generally, practice in this method is conducted when all the trainees are gathered at one site, while organized in one or more groups.

In the practical method, trainees are required to deal with the challenges presented to them through activities as close as possible to those they would experience if these were real occurrences. They do not declare verbally; they **act**. Generally, practice in this method is performed when each trainee operates in their real operating environment. In this method too, the trainees discuss with each other, but this is not limited to consultations and discussions; rather, it is executed based on the means of communication intended for real events.

Table 1 table summarizes the advantages and disadvantages of both methods.

Table 1. The Advantages and Disadvantages of Both Practice Methods

	Advantages	Disadvantages
Theoretical Practice	Inexpensive to perform. Minimal need for aids. Allows focus on the "soft" components of the organization (perception, policy, methodology). Requires relatively short preparation. Simple to manage. Presents a low risk to the functioning of the organization and its systems.	Does not allow the practice of organizational function beyond the level of the individual. The practice is "static" in nature.
Practical Practice	Allows efficient and effective practice of organizational function at all levels, on a large scale, and with great efficiency.	Expensive to perform. Exercise is resource-intensive. Requires long and relatively complex preparation. Complex to manage. Presents a high risk to the organization's systems.

Based on the table above, theoretical practice should be used when:

01

It is the first exercise (ever, or in the relevant field) for the entire organization or for key functionaries in it.

02

The organization examines the need to make a structural change (whether it results from updating objectives or regular tasks of the organization, or not).

03

The organization examines the need to make procedural change, or any other fundamental issue concerning the functioning of the organization.

Practical practice is recommended when:

01

The organization is relatively young but its management estimates that it has reached operational maturity and seeks to examine this assessment.

02

The organization has recently implemented a procedural or structural change and seeks to examine the appropriateness of the change or the success of its implementation process.

03

The organization identifies significant gaps in the effectiveness or efficiency of its function, and seeks to take advantage of the diagnostic potential of the exercise to analyze the problem and learn how to solve it.

Practice Settings

Each of the practice methods listed above can be implemented in specific settings. The setting expresses the way in which the chosen practice method will be implemented. Although the setting should be based on one of the methods described above, it is possible and even common to incorporate components from the other method. The two main settings for performing **theoretical practice** are presented below.

Tabletop Exercise (TTX)

In this setting, the trainees are gathered in one team or more, and each of them turns to one table and conducts a panel discussion on how to deal with the challenges/problems presented to them, usually as part of a "rolling" story. The team structure may reflect a real organizational structure. Alternatively, they may be constructed as think tanks to enable brainstorming and encourage creative thinking in a practice environment free from everyday constraints.

The trainees respond to a scenario to which they are declaratively exposed (usually, these statements are made in the room, but can also be documented in real time as part of the trainees' ongoing discussion). It should be noted that the scenario in this setting is completely simulated (methodical, as it is commonly called).

Since the exercise is an instrument designed to enable learning, the data from the situation report at its end point is of secondary importance. The main importance is the functioning of the trainees, and not the exercise's results.

The main use of the TTX exercise is to increase general awareness of cyberthreats, memorization and internalization of concepts, and validation of operational plans and procedures. It can also be used to identify significant strengths and vulnerabilities in the organization's defense system against cyberattacks. As such, it is particularly suitable for practicing in the organization's operational and strategic ranks.

Due to the characteristics of a tabletop exercise and the circumstances in which it is conducted, controlling its performance is simple. Thus, it is considered an accurate tool, in the sense that it is relatively easy to meet the goals set for it in the first place.

Organizational Game[5]

Similar to a TTX, an organizational game also has a number of teams of trainees who deal with an evolving scenario (simulation). Unlike a TTX, an organizational game is actually a role-playing game (hence its name), in which all participants form a system together: each team typically represents a particular body or organization, or even an entire country.

The interactions between teams and their members are predetermined and may be friendly, competitive, or hostile, and their functioning is driven and controlled by rules that are also predetermined (although some may be hidden from the trainees' knowledge throughout a part of the game or until the end).[6]

Due to the nature and character of an organizational game, and unlike a tabletop exercise, the results of the trainees' performance often have specific meaning and therefore may play an important role in drawing conclusions from the game. From the point of view of the single organization, an organizational game is primarily intended for practicing internal entities at the operational and strategic level in relatively large organizations.

5. It is common worldwide to call an organizational game a war game.
6. Due to the nature of interaction in an organizational game, there is typically a built-in tension between trainees, which stimulates them to think and act (methodically) and creates a competitive atmosphere that aids learning.

The main setting used to perform a **practical** practice is the **operational** exercise, as detailed below.

Operational Exercise

In this setting, trainees operate in their true operational environment, on its components and conditions. Due to its characteristics and the circumstances in which it is conducted, this setting allows practice from the techno-tactical level, where the focus is on personal and team areas of expertise (mainly through hands-on exercises),[7] to the strategic level, where it is a systemic and extensive practice at the intra-organizational and multi-organizational level.

The focus is on decision-making processes, work processes, interfaces between bodies and units, procedures, and policy issues. In operational practice it is possible, however, to use real scenario elements,[8] but this is usually limited and on a relatively small scale.

Without diminishing the importance and necessity of practice at the techno-tactical level, there is no doubt that the maximum realization of the potential inherent in the operational setting is at the operational and strategic level. Therefore, the discussion will focus on these levels from now on. Appendix 4 contains additional details regarding the techno-tactical level.

A key condition for ensuring the effectiveness of an operational exercise is that the combination of trained entities faithfully represents the organization as a whole. The existence of this condition stems from the fact that the whole organization can never be trained, and it means that the lessons learned from the exercise will indeed be relevant to the organization as a whole, even though only part of it is actually trained.[9]

7. Hands-on exercises are intended for functionaries who deal with the technical and technological aspects of cyberprotection—analysis, reverse engineering, incident response, etc. Their effectiveness usually requires the use of dedicated simulations.
8. The intention here is to take real action in relation to the authentic components of the organization, and especially to a real cyberattack on them, or alternatively to any real damage inflicted on them by other means.
9. It is important to clarify that fulfilling this condition does not necessarily mean striving to train most of the organization. In other words, it is a question of essence and quality, not of quantity.

/02. Exercise Folder

An exercise is a type of operation. Therefore, for an exercise to achieve its goals, it must be planned in advance. This program is the **exercise folder**, and it includes the following components:

Exercise outline

Exercise scenario

Exercise news file

The preparation steps for these components will be detailed in order below.

Exercise Outline

The exercise outline is a collection of all the characteristics that determine the nature and character of the exercise, and they are presented below in the order in which they are determined:

- **Goal of the exercise**
- **Composition of trainees**
- **Subgoals of the exercise**
- **Practice topics**
- **Practice setting**
- **Exercise indicator**

The outline should be determined during the construction of the organization's annual or multi-year exercise program. The other components of the exercise folder will be defined near the date the exercise is conducted (see Appendix 1 to this guide).

The goal of the exercise expresses the organization's intention to examine certain components or aspects of its readiness at a given point in time. Therefore, it would be appropriate to define the entities responsible for the existence and preservation of the proper level of said components and aspects as **trainees**. The trained entities are supposed to fulfill this responsibility through a series of regular and dedicated tasks, each assigned a required achievement. It follows that any such achievement is also a **subgoal** for the exercise.[10] The **practice topics** will be derived from subgoals.[11]

An important element in determining the goal of the exercise is the rule of inversion between the means and the goal of the exercise. In real life situations, the organization realizes its readiness to the extent possible to achieve its business goals and fulfill its mission. In an exercise, on the other hand, it is the level of organizational readiness that is the focus of interest, and the exercise is intended to examine the extent to which said level of readiness has the power to enable the organization to achieve its goals and mission. In other words, the exercise goal focuses on examining the organizational means (the "how"), while the goals and mission of the organization (the "what") are expressed in the exercise indirectly, using the same regular tasks mentioned above, and the organization determines a required achievement for each one.

10. It should be emphasized that the exercise must have one and only goal, and in accordance with the saying "grasp all, lose all," it is recommended to deduce a maximum of three subgoals.
11. Following on from the subgoals, it is recommended to define a maximum of three practice topics.

As stated, exercise is not fundamentally a judgmental activity. At the same time, it is obvious that the achievements of the trainees are essential information for achieving the goal of the exercise, since it will only be possible to assess the readiness state of the organization based on them. The trainees' achievements should be evaluated according to **the competency and readiness indices** defined in the organization for the relevant areas of operation. Therefore, the exercise folder should include a collection of all the relevant indices for the purposes of the exercise and the topics of practice derived from them. This collection is called the **exercise indicator**.

The use of these indices is not an exact science; therefore, they must be carefully measured and evaluated. There are various tools that can help minimize the degree of bias in the situation report of competence and readiness obtained at the end of the process (e.g., reliability between judges), but this is not the place to expand the discussion in this wide-ranging professional field.

The construction of an outline for a particular exercise is not self-sustaining. Each exercise should be a link in a continuous chain of such performances, whose purpose is to maintain, preserve, and promote organizational readiness to deal with cybersecurity events and crises. This directly affects the determination of the level of requirements each exercise places on the trainees (optimally, each exercise places higher demands than its predecessor). A key element in designing the outline of a given exercise is the conclusions from all exercises performed prior to it.

While the outline expresses what the organization is interested in learning from the exercise, the component of the exercise folder that actually enables this learning is the **exercise scenario**.

Exercise Scenario

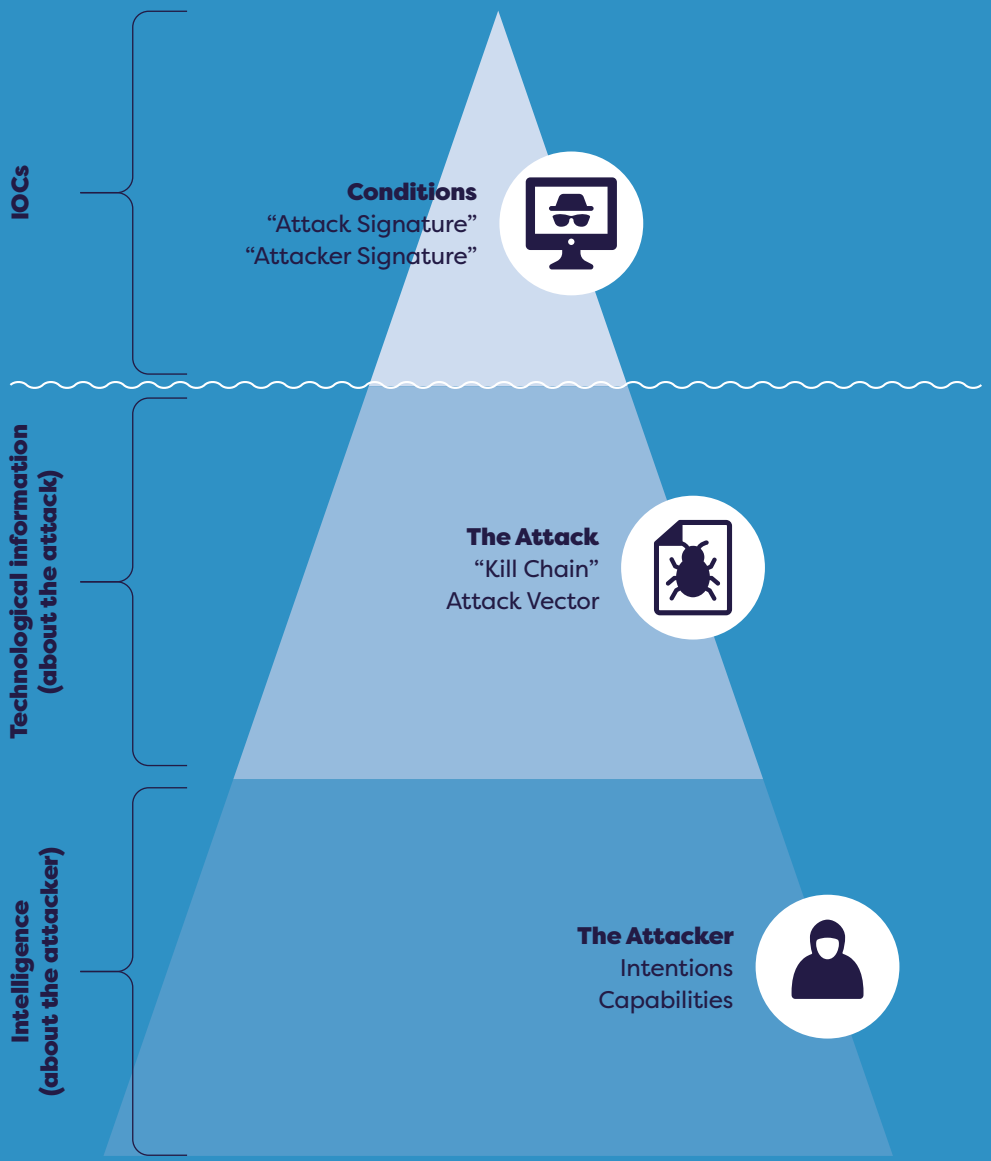
The scenario is the "plot" of the exercise, and what happens during it are the stimuli that the trainees are supposed to respond to.[12] The scenario should be realistic, plausible, and challenging. The fundamental building block of the scenario is a **cyberattack**. A scenario may contain one or more attacks, but the total number of attacks should not exceed five. **By definition, each exercise has only one scenario.** At the same time, the scenario may be constructed as a series of plots, each of which stands on its own. In such a case, each plot will contain at least one cyberattack.[13]

Figure 1 below shows the Iceberg Model—a model of cyberattack—from two angles: that of the attacker and that of the defender. From the point of view of the attacker, the attack is a move designed to achieve a defined goal that serves their intentions while utilizing their abilities in the field. The attack produces various visible effects, which occur within the defender's systems and are manifested in disruptions in their function and often also in other visible signs, indicating its existence (various "signatures"[14] of human players and means involved in the attack).

From the point of view of the defender, it is exposed to a series of indicators of compromise (IOCs) indicating the possibility of a cyberattack. These include all the effects and signs mentioned above (since they are visible to the defender). However, it is expected that for the defender many of them will be out of context, since they indicate an activity that by its nature is done secretly.

12. The following is valid for all practice settings.
13. This type of scenario is mainly suitable for theoretical practice (tabletop exercise or organizational game). In practical practice it is crucial to visualize a possible reality effectively, and therefore the most appropriate scenario for this purpose is one continuous plot.
14. The term "signature" refers to information related in one way or another to the actions of the attacker that is revealed by the defender (such as interception of a reference made in a darknet discourse to the organization or its unique cyberasset, or a port scan performed frequently on its particular cyberasset).

Figure 1. The Iceberg Model



These signs are represented in Figure 1 in the form of the tip of the iceberg (its "top ninth") floating on the surface of the water, visible to the naked eye. All the other information about the attacker and the attack, which is immersed in the depths of the attacked cyberspace, is depicted in the form of the other eight-ninths of the iceberg, submerged and hidden from sight.

Therefore, from an exercise point of view, this information is secret, and its details will be known to the trainees (i.e., the defenders) in two cases only: one, when the trainees deduce them on their own based on the news they received, and two, when they are exposed to the trainees on the exercise directors' initiative.

The exercise dynamics are summed up in the trainees' efforts to successfully overcome the challenges presented in the scenario, while constantly dealing with a lack of information, irrelevant information, and ostensibly contradictory news. These dynamics exist on two levels: the operational level (organizational processes—operational, business, or other) and the technological level (processes that take place within cyberspace). Of course, there is a strong affinity between the two, since the purpose of the organization's information and communications technology (ICT) infrastructure is to support its operational processes, and when these are attacked, the operational processes will be compromised.[15]

This dual situation forms the basis for operational dilemmas to be formed (not only in the exercise, but also in real life). For example, the organization's chief information security officer (CISO) may recommend that management proactively disable a particular operational process to reduce the organization's "attack surface" in view of possible developments of the attack already taking place. Management, for its part, may oppose such a move out of a clear business interest.[16]

15. This is valid for both the IT world and the operational technology (OT) world.

16. In this context, it is worth mentioning the importance of risk management during a cybersecurity crisis, and in the process assessing the impact of a cyberattack on the organization's business processes (called a BIA, or Business Impact Assessment).

To ensure that the exercise achieves its goal, the challenges that the scenario will pose to the trainees should arise from the practice topics. Trainees should be encouraged to act in areas directly related to the subgoals of the exercise.

Figure 1 depicts a partial picture of the scenario's structure. In the reality of the cyberdimension, what appears to be the tip of an iceberg protruding above the surface of the water may turn out on closer inspection—that is, after proper investigation—to be a mound of foam carried on top of a large wave. And in less picturesque language, not everything that appears to be a cyberattack is indeed such.

In light of this, and in order to build a simulation as close as possible to reality, innocent events (such as system malfunctions or operational faults) should also be included in the exercise scenario. In the vernacular of exercises, this component is called "noise."

Creating the Exercise Scenario: Guiding Principles

01

The weight of the cybercomponent in the exercise: The scenario should present the trainees with a challenge in the area of cyberprotection throughout the entire exercise, without excluding the importance of the operational aspect of the exercise.[17]

02

Realism: The scenario should reflect to the trainees the reality known to them, down to the smallest detail. This applies not only to information about the events in the exercise simulation, but also to the developments that take place in it as a direct result of the trainees' actions during the simulation. This is necessary to ensure that the trainees trust what is being told to them and as a result feel empathy with the evolving situation in the exercise and function "naturally" within it—that is, in a way closest to how they would act if the events described were happening in reality. For this reason, it is recommended to involve in the planning process representatives of the trained organizational units who have expertise in the issues of practice.[18]

03

Severity: This is the severity of the general state of the organization as a result of the cumulative damage caused by the cyberattacks included in the scenario. From the outset, the construction of the scenario should take into account the outcomes of the risk assessment process and their analysis performed by the organization.[19] In this view, the "center of gravity" of the scenario will be based on those attacks included in it, whose damage expectancy is estimated to be high. Within these, it is important to have at least one scenario which is estimated to have a low probability of actually occurring.

04

Difficulty: Human experience shows that failures motivate learning far more than successes.[20] Therefore, the scenario should be constructed to be significantly difficult for trainees such that their chances of at least some of their efforts failing is almost certain. On the one hand, the difficulty level of the scenario should be high enough to take the trainees out of their comfort zone, and in this way motivate them to strive to deal with the challenges it presents, but it must be low enough to not have the trainees frustrated in the face of the challenges the scenario holds, which would ultimately diminish their motivation to invest such efforts.[21]

17. An extended discussion of this matter is provided in Appendix 2.

18. Such experts will be prevented from participating in the exercise, as they have been exposed in advance to the details of the scenario. It is better to deal with the dilemma "trainee or confidant in the exercise?" before the exercise, than to face a fait accompli when conducting it.

19. There are different approaches to assessing the risks posed to the organization (regardless of the cyberfield specifically). This is, of course, a very important subject, but dealing with it goes beyond the scope of the discussion in this guide, and therefore will not be expanded here.

20. In this context it would be appropriate to quote Winston Churchill's famous saying about the importance of failure: "**Success** is all about going from **failure** to **failure** without losing enthusiasm."

21. Keep in mind that there is a connection between the severity of the scenario and its difficulty.

05

Background story: So far, the discussion of the scenario has been based on the assumption that it will be revealed to trainees only when the exercise is conducted. Without contradicting this, it is possible to publish a background story prior to it. This would be a collection of news items, some of which contain information regarding the cyberattacks that will take place in the exercise, and some of which are "noise." In any case, the background story will not contain information already included in the scenario.

The idea behind this component, which is optional, is to encourage the trainees to start preparing for the exercise itself and to create tension and anticipation among them. Therefore, if a background story is used, it should be distributed to trainees about a week before the exercise date. By definition, the background story is an integral part of the exercise outline although, as mentioned, it is published at a separate time.

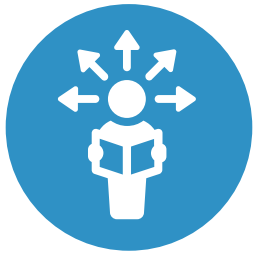
06

Exercise distortions: Even if all the above orders are fulfilled, one limitation remains that the best scenarios cannot avoid: no simulation can be a perfect substitute for reality. It follows that in each exercise there will be certain distortions in relation to what is expected to occur in identical circumstances in real life. The most significant damage inherent in these distortions is that they threaten the validity of the lessons to be learned from the exercise. Therefore, the scenario needs to not only most faithfully express the challenges that trainees are supposed to face, but also must roll out in a way that reflects the reality in which they are accustomed to operating in day-to-day life.

The Exercise News Items

Based on what was described earlier, the exercise scenario is nothing but a collection of "icebergs" created by the planners of the exercise, with the virtual reality within which the trainees will have to function based on a collection of signs that form the visible surface of each iceberg. This is not enough, however, because as stated above, in real life it is likely that trainees will be exposed to additional items of information about the attacks and the attackers who cause them.

Thus, the scenario undergoes a process of breakdown, during which both its visible part and details of its hidden parts are processed into a collection of **exercise news items**.



The resulting **exercise news file** expresses both the cyberattacks and the noise events included in the scenario. As stated, while the creation process of the scenario is done from the point of view of the attacker, the process of breaking down the exercise news items is done entirely from the point of view of the defenders—that is, the trainees.

An exercise news item is an information record with a fixed structure, which comes in two configurations: limited and extended. In its limited configuration, an exercise news item includes the following fields:

01

The individual that **conveys** the news: a person who is a part of the practice, or not.[22]

02

The **recipient** of the news item (trainee, by definition).

03

The **exercise date and time** at which the news item is delivered to the trainees.

04

The **real time** of delivering the news item to the trainees.

05

Content of the news item.

22. Under no circumstances is this person the exercise director or any of their assistants. Individuals are only taken from the real operational environment of the trainees. As mentioned, some may participate in the exercise themselves. The rest will be presented by participants deployed by the exercise director, who belongs to the exercise management team.

An exercise news item should:

01

Faithfully express the effect that is supposed to be created at the point in time discussed in the process of unfolding the cyberattack/the exercise "noise" event.

02

Not include any information that is an exercise secret.

03

Faithfully express the information flow process that is predicted or expected to take place in the event of a real occurrence.

The general dynamics of an exercise can be described as a journey the trainees take to the insights and lessons learned at its end. Although essentially the content of the latter is not known in advance, the exercise directors know very well where, in general, the trainees should get to at the end of this journey—the goal of the exercise, its subgoals, and the topics of practice should clearly express that. In this view, the news items provided to the trainees are the means the exercise directors have to motivate the trainees to carry out this journey and to guide them on their way so that they will indeed reach the desired destination.[23]

At the same time, the exercise directors cannot control the trainees' response to the news items; therefore, there may be a situation where the trainees stray or simply get stuck in it without the ability to move forward. In such a case, the exercise directors have at their disposal a special type of news item: **guiding information**. Guiding information does not have a pre-planned delivery time. It is kept ready in case of need, and when the need arises it is handed over to the trainees. Guiding information is an organic part of the scenario and plot of the exercise. The expectation of the exercise directors is that the information it provides will help the trainees to progress as required.

Sometimes, however, even this measure is not enough. In such a case, direct intervention of the exercise directors in the trainees' actions will be required in order for them to advance.

23. In general, there should be no direct dialogue between the exercise directors and the trainees during the exercise. More about this in the discussion on managing the exercise, later in this guide.

Exercise News File, Trainee Responses to the News, and the Exercise Clock

The exercise news file is a table or spreadsheet in which each line is dedicated to one exercise news item. As can be understood from the above, this file should be a structured chain of messages, faithfully expressing the development of the events included in the scenario (both attacks and noises), and it should also take into account the trainees' expected responses to the events. This will aid the exercise directors to control the exercise's development and moves.

To assist in such control, the reactions of the trainees to each news item must be mapped in advance. A distinction must be made between a **desired** and an **expected** response. The desired response expresses the proper and correct way of dealing with the stats presented by the news item (a "by-the-book solution"). The **exercise indicator** may help a lot in determining it. The expected response, however, reflects what the trainees are likely to do in practice and is based on the exercise directors' familiarity with the trainees and with the existing situation as a whole.

It is not necessary to fill in these two fields for each news item. Sometimes, it would be right and appropriate to express a significant change in the exercise situation report through a sequence of several news items, which only at the end of it (i.e., in the last news item) would it make sense to define the trainees' responses to the new data provided to them.

Based on these responses, the news items are arranged in the exercise news file in their **extended configuration**, which contains two additional fields compared to the limited configuration:

01

The desired response of the trainees to the information.

02

The expected response of the trainees to the information.[24]

The need to control the course of the exercise and its development also requires the "exercise clock" to be addressed when compiling this file. The exercise scenario may depict a simulated reality that occurs on a date and time different from those actually taking place (real time). The date and hours set in the scenario are, therefore, referred to as the exercise clock. It is expressed in practice in the timing of the news.

For the most part (and certainly when it comes to cyberattacks), the real amount of time allocated for the exercise is significantly shorter than the length of time over which the events in the exercise would take place in reality. To overcome this difficulty, it is necessary to shrink the real time that would have been required to respond in reality to the events in the scenario, and to allocate trainees significantly shorter time frames to respond to the news items they receive.

Thus, the news items have two schedules: one reflecting the "exercise date and time of delivering the news item to the trainees," and a second schedule with the "real time of delivering the news to the trainees." (For example, trainees can be given two consecutive news items half an hour apart in real time, while the events described in them happened in the exercise twelve hours apart.)

The constant gap between the two time scales discussed here (which is even expected to increase as the exercise continues) may have the trainees feeling that the advancement of the exercise clock is "jumpy." Therefore, exercise directors should strive to keep these transitions as smooth as possible.

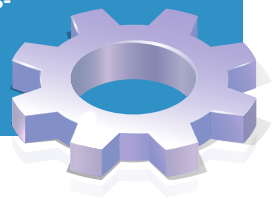
24. For the record, the exercise news file is used by the exercise directors to control the exercise's moves, and its content is not disclosed as such to the trainees. The news items it contains are actually transmitted to them in their limited configuration (i.e., without the "desired response" and "expected response" fields, as stated above). Technically, they can be transmitted by various means, both manually and mechanically.

As for the degree of shrinking, one should take into account the (real) period of time appropriate to allocate to trainees in order to respond to every news item. Allocating too short a time frame may impair the effectiveness of the practice and, therefore, should be avoided.

In this context, it is befitting to discuss the common tendency of exercise directors to load tasks on trainees to examine their functioning under stress. It must be said, first of all, that stress is not necessarily a consequence of the **amount** of information that trainees have to deal with, but of the **meaning** of this information, and therefore, one should focus on designing the news items' content properly and not on their amount to achieve this purpose.

Beyond that, functioning under stress is a basic and especially personal skill, and therefore practicing it is relevant mainly to the practical method—that is, to the operational exercises, and more precisely (for methodological and didactic reasons) to those conducted at the techno-tactical level of the organization. But in this case the gap between practicing this skill and building it is quite small, and therefore it is advisable for the organization to address it through training activities (such as, for example, combining it in executive training).

A big rule in the world of exercises is to never automatically copy an existing exercise folder in order to conduct a new exercise. Practice is one of the most effective ways to force an organization to step out of its comfort zone and thereby reduce the risk of perceptual fixation and the transformation of common behaviors into sacred patterns.



/03. Managing the Exercise

Exercise Administrative Division and the Organization's Exercise Unit

So far, the term "exercise directors" has been used in the guide. Indeed, an exercise is not created or conducted on its own. For this purpose, there is **an exercise administrative division** (the administrative division). The administrative division of an exercise conducted in the cyberdimension stands on four legs:

- **A methodologist** (who often also serves as the head of the division)[25]
- **A technologist** (who is also responsible for intelligence on the attacks)[26]
- **A process specialist**
- (In some cases) **An intelligence specialist** regarding the attackers[27]

25. It is usually expected that the head of the organizational exercise unit will serve as the head of the administrative division. At the same time, and mainly for representative reasons, a more senior employee from within the organization will be appointed to this position.
26. This refers mainly to what is known in our circles as "blue intelligence"—that is, to information that is mainly technological, and in the context of the cyberdimension, mostly handled by both the organizations subjected to cyberattacks and commercial cybersecurity agencies (local and international) who specialize in it.
27. This refers to "red intelligence," or information that is under the responsibility of the national intelligence community. Although nowadays the boundaries between these two worlds of intelligence are often blurred, community elements still have, of course, significant unique capabilities.

Usually, the exercise administrative division will include additional functionaries; therefore, the four above-mentioned functionaries will be referred to hereinafter as the **leading team** of the exercise.[28]

The term "administrative division" refers to a dedicated and temporary organizational entity that is established prior to conducting a particular scheduled exercise set out in the work plan and disassembled when the process of drawing conclusions from it is completed. For the purpose of constructing the organization's annual exercise program (which includes the outline of each of the exercises set forth in it), a small team, comprising one or two people, is sufficient.

Hence, it is befitting that the small team should constitute a permanent unit of the organization, which would be responsible for managing all its practice activities on an ongoing basis. Hereinafter, the guide will refer to this unit as the **exercise unit** (of the organization) to distinguish it from the body known as the "exercise administrative division." In this view, the exercise unit will form the nucleus around which the administrative division for each specific exercise will be formed.

In general, the administrative division simulates any functionary or body or organization that does not actually participate in the exercise. To prepare in advance for a response to expected, and especially occasional, developments in the course of the exercise, these can be represented through pre-prepared news items. This rule can be put into practice in many cases of theoretical practice. In practical practice, however, possible developments during the exercise may require advance preparation of a large number of such news items.

Moreover, the need for their properly timed delivery to many trainees within a short time frame can create an unbearable burden for the administrative division. Therefore, it is recommended and also customary to use dedicated functionaries, or **agents**, for this purpose during the exercise. The agents are real functionaries from both within and outside the organization being trained. In the exercise, it is their job to represent themselves or their organization. They can be divided into two subgroups: those over whom trainees have some authority or who are internal or extra-organizational colleagues, and those who have authority over the trainees (for example, in an exercise designed for company management, the first group may include various employees of the organization being trained and the second group may include the company's board of directors, untrained senior executives, or some state regulator).[29]

Since there are certain similarities between the activity of an agent and that of a trainee, it makes sense that an agent may also be rewarded for the exercise, even though they were not among the trainees, in the form of a bonus. Either way, the agents are members of the administrative division for all intents and purposes.

In monitoring the trainees' actions, the administrative division is assisted by **lookouts**. A lookout is physically present in the practice environment and observes the moves of the trainees operating in it. Lookouts perform two roles: in the course of the exercise, they are a regular link between the administrative division and the practice environment, and after its completion, they prepare a concluding report on the trainees' performance throughout the exercise. Like the agents, the lookouts are regular members of the exercise administrative division.

28. From the outset, the unique characteristics of cyberspace place considerable limitations on the ability to include in the scenario real intervention actions, both at the initiative of the administrative division and at the initiative of the trainees. At the same time, the administrative division should consider the appointment of a **safety controller**, who will oversee the actual activity that takes place during the exercise, and prevent the formation of circumstances that could endanger the organization's cyberspace in any way.

29. In common parlance in the field of exercises, these functionaries are usually referred to as "low control" and "high control," respectively.

As noted above, the leading team and the lookouts should not interfere with the trainees' actions. In fact, the administrative division should try to be as transparent and imperceptible as possible to them. There are two exceptions to this rule:

01

As already explained, if the administrative division has not been able to direct the trainees' actions according to its plan at a certain point in time, even after using guiding news items, there is room for its direct intervention in the trainees' function for this purpose. In this context, the administrative division strives to achieve the goal of the exercise, and not necessarily to deliver all the news items it has prepared for the trainees by the end of the exercise.

02

The trainees may contact the administrative division with questions regarding the management rules of the exercise (for example, regarding the exercise clock, the role that a particular agent plays, etc.).[30]

30. Differently, and according to what has already been explained, it is expected and predicted that the trainees will be in regular interaction with the **agents**.

Practice Environment

The practice environment is where the trainees operate. There is a fundamental difference between the practice environment used for theoretical practice and that used for practical practice: in practical practice the ambition is, as stated, for the trainees to operate within their real and natural operating environment. It also follows that the practice surroundings will typically span over several sites, some of which will contain more than one functional space. On the other hand, in theoretical practice, the aim is to create conditions that encourage thinking free from everyday constraints. Therefore, it is common that trainees operate in this framework in an artificial environment, whose design is guided by didactic and logistical considerations, so that in most cases it has no connection to their real operating environment.

It will usually contain one space—the hall or the room where the exercise will take place. If practice includes teamwork, the practice environment will include additional work spaces. Another consideration that has an impact on the design of the theoretical practice environment is information security—that is, the level of security classification of the exercise material. Thus, it may be necessary to create secluded practice areas that will allow partitioning between different work teams.

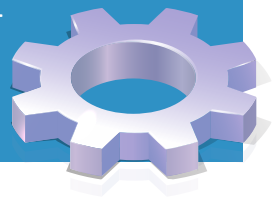
Another difference between the two methods of practice in this regard is the weight and significance of the means of simulation. In practical practice it is natural to want to carry out an actual cyberattack on the organization's ICT systems. Unfortunately, this aspiration is limited by legal, safety, material, economic, and image considerations. The seemingly obvious solution to this problem is to use a separate and dedicated ICT infrastructure or network environment for practice purposes that faithfully mimics the structure and functioning of the organization's true ICT infrastructure.

Such a solution is usually expensive and requires constant maintenance and updating to continue to faithfully represent any change or update in the real organizational cyberspace. Beyond that, its effectiveness will be limited since there is really no practical possibility to simulate all the business processes that rely on this infrastructure. In many cases, this will require the establishment of an entire dummy organization.

Thus, in the absence of such simulation infrastructures, practice in the real environment often requires not only limited use of its components and resources, but also use of components and means separated from it and used for practice purposes only. This is a principle of action known as "separating the practice environment from the real environment." Therefore, in an operational exercise, the administrative division must take special care in designing the exercise news items to help illustrate the attack and its consequences, ensuring as much as possible that the exercise image based on them will compensate, even partially, for distortions such compromise will create in the practice environment.

By its very nature, theoretical practice places more modest demands in this area. In fact, in this case it is more about "giving color" than simulation—that is, giving as authentic a character as possible to the occurrences described in the exercise news items. Thus, for example, news items can be colored to a considerable extent by screening a newsflash produced especially for that purpose in the room where the exercise is held.

The use of simulation and illustration aids is intended to enhance the authentic impression that the exercise situation makes on the trainees, in order to encourage them to function naturally, as opposed to giving the exercise an impressive appearance. Since such aids are a relatively expensive resource, it is advisable to avoid using them as much as possible just for creating pyrotechnics and to limit the investment in them to specific cases in the scenario that justify it.



Safety in the Exercise

Without contradicting the above, the exercise administrative division must carefully examine the exercise scenario and the exercise news file from the aspect of **safety**. If the administrative division comes to the understanding that playing out the scenario may create circumstances in which there may be some risk to the organizational cyberspace (which may damage organizational cyberassets and possibly even result in incidental damage), then a **safety controller** should be appointed for the exercise.[31] The safety controller will prepare a **safety appendix** for the exercise outline, which will include a series of instructions aimed at all participants to prevent the above risks from developing and to instruct participants how to act in case any risk materializes nonetheless.

Technical and Logistical Preparation of the Practice Environment

Theoretical practice differs from practical practice in the technical and logistical aspects. This matter is discussed in detail in the appendices to this guide. However, these two settings also have common features in this context, as detailed below:

01

The exercise should be recorded (on video or audio). After the exercise, all the recorded material should be reviewed, and all the information needed to investigate the exercise should be extracted from it. It is advisable to do this within a week from the date of the exercise.

02

Avoid food and hot drink facilities in the exercise space to minimize distraction among trainees. Light refreshments can be placed outside in an accessible place. In an exercise that takes half a day, a light lunch should be provided. In exercises that last a few days, make sure that providing food to the participants does not interfere with the exercise. Provide food and drink proactively and in a planned manner.

03

Access to the exercise arena is extremely important. Send participants directions on arriving by private car and public transportation about a week before the event, with information regarding parking arrangements.

04

Occasionally, conducting the exercise will require dedicated security services, both physically and regarding information security. The administrative division must include an orderly security plan in the exercise folder and ensure its implementation while the exercise is being held.[32]

31. In any case where such risks are recognized, the administrative division must carry out a risk analysis process and determine the final configuration of the scenario and the exercise news file according to its results. In addition, the process of approving the exercise outline will include approving the safety preparations for it, while paying attention to the appropriate emphases.

32. Together with the security aspect of the practice, it also has a safety aspect. Since the cyberattacks in the exercise are supposed to be simulated, and in light of the fact that in the first place it is necessary to separate the practice environment from the real environment, the safety aspect is manifested especially in the case of physical activities involving safety risks.

Briefing the Trainees before the Exercise

An exercise is a kind of game. As such, it is performed in a defined "arena," according to pre-determined rules. Therefore, it is very important that the trainees are well acquainted with the exercise arena and its rules before the date of the exercise.

For this purpose, the administrative division should brief the trainees. The briefing should underscore that the exercise is not a judgment tool.[33] The timing of the briefing and its emphasis depend on the practice method:

01

In theoretical practice, a short briefing is given at the beginning of the exercise. Up to 15 minutes is sufficient. During the exercise, publicly present the participants (mainly those sitting at the practice table, in case there are additional participants who are participating remotely). It is important to go over the full schedule of the exercise, and in case it is held in two or more locations, this should be noted when explaining the rules of the game.

02

In practical practice, where there is usually a physical/geographical dispersion of the trainees, a video conference makes it possible to overcome the time and space constraints and to conduct the briefing at the beginning of the exercise. If this means is not available, a conference call can be made, although it is advisable to preface it with a face-to-face briefing about a week before the exercise takes place. If it is possible to gather all the trainees in one place, one briefing is sufficient; otherwise, several such briefings should be held. In the briefing prior to a practical exercise, the means of communicating during the exercise should be explained, as well as the rules for separating the practice environment from the trainees' real operating environment.

33. In this context, it is common to define the practice environment as a "no-fault environment."

/04.
Debriefing the Exercise and Drawing Conclusions from It

The Debrief: In Theory

Human forgetfulness threatens the survival of any undocumented piece of knowledge, and its effects are immediate. This is accompanied by another human tendency, which is to creatively re-create the past. Thus, the process of drawing conclusions from the exercise should begin immediately upon its completion. The first step in this process is the **after action review (AAR)**. Debriefing is an essential learning tool for any activity; therefore, this chapter begins with general statements concerning it.

The AAR is an investigation of the performance of a particular activity in light of its goals, results, and the processes that were undertaken, with the aim of extracting the most knowledge and data to create a basis for drawing conclusions and learning lessons. There are two types of AARs: **in-house** debriefing and **expert** debriefing.

An **in-house debriefing** is conducted on behalf of the body that was responsible for the investigated activity, and only those functionaries who took part in it in any way participate. Its purpose is to extract as many insights as possible that emerged from the activity, and to do so in a closed and friendly environment, which will allow for an open and free discourse.

It is very important to conduct the in-house debriefing as close as possible to the end of the investigated activity, in order to capture the most important things related to it as close as possible to the time of their occurrence.

Thus, it is customary to conduct a preliminary debriefing called a “hot wash” immediately after the end of the investigated activity. In-house debriefing has two main advantages: first, the information discussed in it is based on the experiences of those who were closest to the investigated activity, and second, the lessons learned based on this information will directly serve those who need to prepare for the next activity.

As such, in-house debriefing is an irreplaceable organizational and personal learning tool. However, it has two limitations: first, even in the friendliest discourse atmosphere, elements may be lacking, or a distorted interpretation may be drawn. Second, the participants in the debriefing are not necessarily experts in the content areas being researched.

In light of this, in many cases it is customary to add an **expert debriefing** to the in-house debriefing. This type of debriefing is conducted by professional experts on issues selected by the body that carried out the investigated activity. None of these experts participated in the investigated activity.

While an in-house debriefing is essential, the decision to conduct an expert debriefing is at the discretion of the investigated body. In the event that the investigated activity concerns a large organization or several organizations, an in-house debriefing in a graduated format is recommended. Each organization or body that participated in the activity investigates itself and reports its investigative results to the position in charge.

When the organizational scope is limited or there is insufficient time, it is still possible to conduct an investigation in a unified format, in which all the relevant parties conduct the in-house debriefing together. The hot wash mentioned above does not replace an orderly in-house debriefing, whether it is done in a graduated or a unified format.

This is valid for any activity whatsoever. With respect to an exercise, two distinct characteristics should be noted. First, with regard to the hot wash, it is important to say that the members of the administrative division are allowed to participate, but their active contribution to the discussion should be limited to sharing details regarding the exercise scenario and how it actually played out during the exercise (this is mainly information that was defined from the beginning as an "exercise secret," so some part of it remains hidden from the trainees even at the end of the exercise).

It is not the role of the administrative division to criticize the trainees' performance, and except for the exception noted earlier, it should refrain from interfering in any way in the investigation processes of the exercise.

Second, the exercise administrative division, like the trainees, is required to conduct its own orderly debriefing. Its interest is to examine the extent to which the exercise met its stated goals. This debriefing should also be conducted internally and without the participation of the trainees.

The Debrief: In Practice

Debriefing the exercise begins as early as the time the exercise takes place. Its first step is to gather most of the information accumulated throughout the exercise and have the trainees document it. This includes records produced by automated systems or communication networks, as well as written records, such as operational logs, reporting forms, and so on.

Documenting this information is a necessary condition for the process of learning from the exercise.[34] Naturally, the raw information collected may contain inaccurate data, and other items that may be accurate but not relevant to draw conclusions from. Thus, the next step in the debriefing process is to verify the data collected, filtering out any incorrect or not reasonably verifiable data. The data remaining in the process after this step is defined as the **facts**. Next, a determination is made about which of the facts are relevant for drawing conclusions. Those that are not are filtered and kept in a separate cache, since they may be relevant in other contexts—practice or real, contemporary or future.

The facts remaining after this stage are defined as **findings**. In the final and crucial stage of the debriefing process, the investigators must combine the findings into a consistent and complete description of their moves throughout the exercise. The combination is made on the basis of identifying links between the findings, mainly of the "cause-effect" type: for example, "finding X produced finding Y." Another type of link is the simultaneous occurrence of different findings, or the occurrence of identical findings at different times. For example: "Finding X occurred at a certain time in a certain organizational cyberasset, and two hours later, finding Y, identical in essence and signs, occurred in another organizational cyberasset."

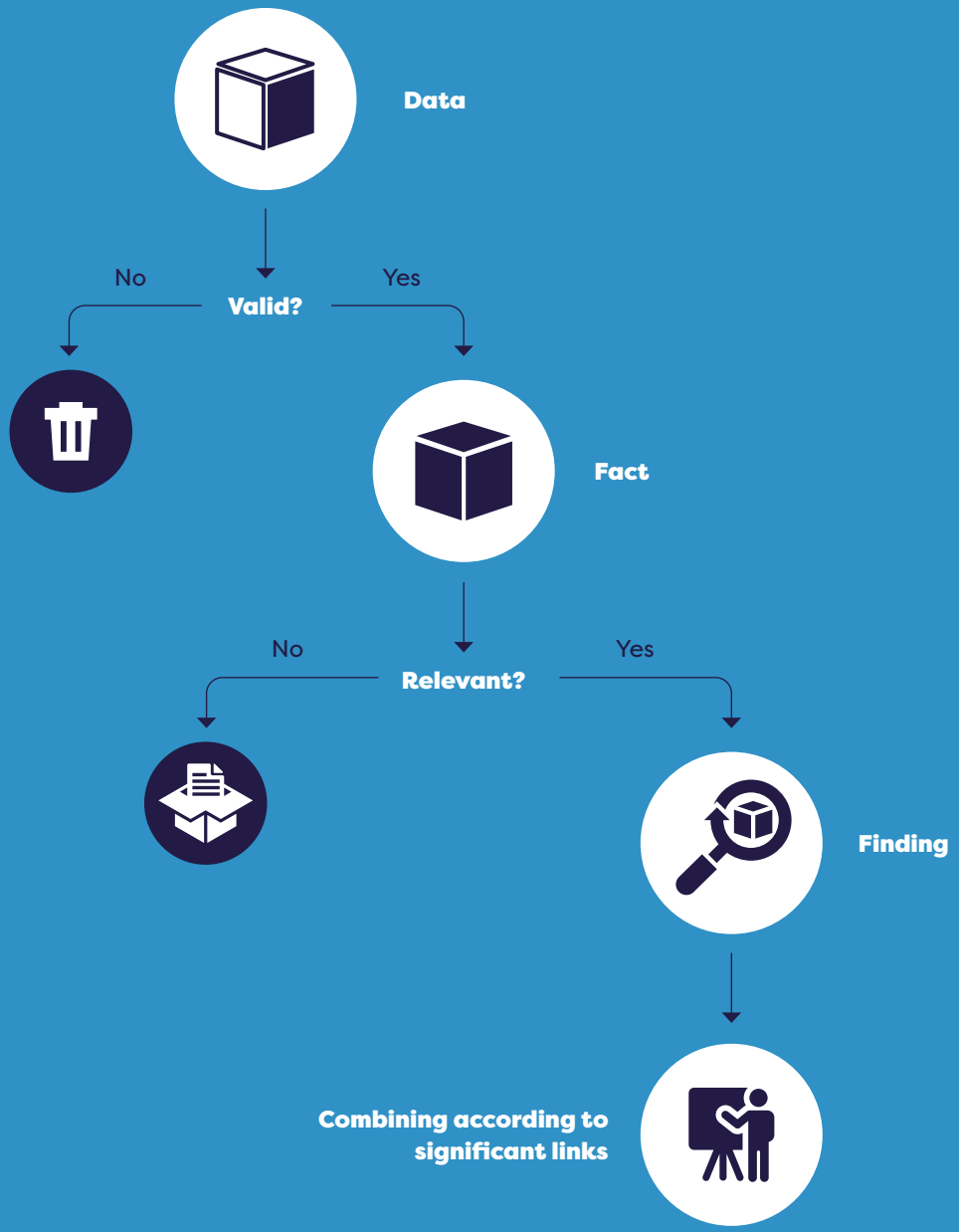
The fact that the organizational cyberspace is, by definition, an aggregate of assets facilitates the creation of significant links between the findings pertaining to these assets. Figure 2 illustrates the debriefing process.

An attempt should be made to create a picture obtained from the combination of the findings that is acceptable to all the participants in the investigation, which is an important measure of its reliability. Thus, this product, called the "exercise picture," should receive the approval of the most senior authority within the organization that participated in the exercise.[35]

34. In this regard, the realization of this condition depends, essentially, on the organizational culture of the trainees having a pan-organizational strategy. Relevant questions include, What is the mission of the organization? What are its goals? What are its regular tasks? What is the general approach to their implementation? How do you ensure the preservation of the existing capabilities of the organization? What steps should be taken to ensure the relevance of the organization to its target audience? and so on. It is also important to have organizational operating concepts, such as in-house, cross-organizational and inter-organizational work procedures, etc. This matter places the effectiveness of organizational practice in a broader context.

35. The point of this confirmation is to state officially that the exercise picture is a faithful description of what happened throughout the exercise. The intention is not to describe the exercise and debriefing process in detail.

Figure 2. The Debriefing Process



Drawing Conclusions

Once the exercise picture has been summarized and approved, its formation throughout the exercise can be examined, according to pre-determined indices. At this point, a key pair of questions are asked: Why did what happened happen that way, and should (in the given circumstances) it have happened differently? The answers to these questions are the insights that will serve as a basis for drawing conclusions from the exercise.

Not everything that emerges from this is necessarily new. However, long-known insights are also important, as their exposure increases their validity and helps to establish conventions on which the future functioning of the organization will be based.

As an extension of that, new insights are something to be welcomed, but also to be treated with caution: the circumstances from which they arise may have been coincidental. Moreover, this is an exercise, so it is possible that without the exercise simulation, this coincidence would not have occurred.

The main part of this guide noted the importance of failure as a learning tool. In the context discussed here, therefore, it should be noted that the successes as well as the failures of the trainees are important to debrief.

Just as it confirmed the exercise picture, so too must the organization's management approve the list of insights formulated. An approved insight is defined as **a lesson**, and as such, it has a binding status in the organization. Below is a list of the key components of organizational readiness that the lessons can address:

01

Work plans and procedures of the organization.

02

The organizational structure of bodies in the organization or of the organization as a whole.

03

The management processes of the organization (the "information flow" processes in the organization and the decision-making mechanisms based on them).

04

Organizational resources (manpower; ICT systems such as hardware and software; other systems; logistical means; budgets, including scope and distribution, etc.).

In the vernacular of many organizations, it is customary to distinguish between a "lesson for preservation" (i.e., an insight that points to a strength that should be preserved) and a "lesson for improvement" (i.e., an insight into a point of failure, weakness, or lack that requires correction). This act of approval is of great importance since a lesson not only teaches something about the organization and its function; it also contains a duty to act as a result.

In other words, a lesson learned is meaningless unless it is applied. Thus, the lessons learned must be translated into tasks, and incorporated into the work plan of the organization. Since learning is a circular process, the manner in which the lessons are applied and their actual results need to be re-examined in future exercises, which are also designed to learn and apply lessons, and so forth.

Process Documentation

Upon completion of the conclusion-drawing process, the organizational exercise unit will publish a report to the organization's management, to all the trainees, to the exercise administrative division, and to any other factor concerned, which will include:

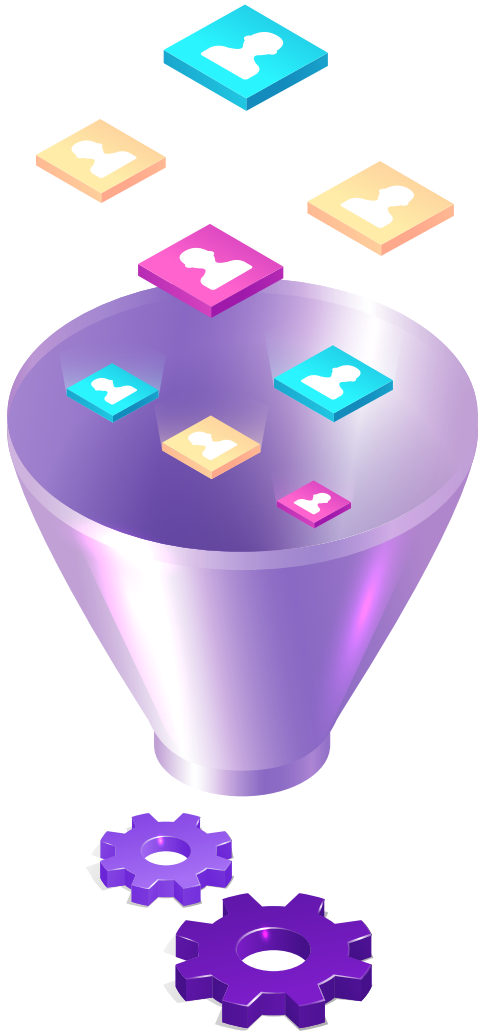
- **Exercise outline.**
- **The actual course of the exercise:** Key points worth noting.
- **Exercise lessons:** This component will include assigning a body responsible for applying each lesson. These are not work plans for applying the lessons; those will be prepared and published by the bodies responsible for their implementation.
- **Lessons learned by the administrative division:** Insights about the exercise itself (the exercise folder and how it was applied in practice) and actions that the organizational exercise unit intends to take to inform the organization's future exercises.

Appendices

Overview

In line with what was explained at the outset, the main part of this guide focused on defining the terminology of the world of practice, emphasizing practice in the cyberspace dimension. The following four appendices cover actions that the organizational and administrative exercise units of each exercise must perform for the purpose of creating and managing cybersecurity exercises.

Accordingly, they focus on selected issues that require further deepening and detailing and should be read only after reading the main part of the guide.



Appendix 1. Guidelines for Building a Cybersecurity Exercise Outline

The Exercise Outline and the Organizational Exercise Plan

The exercise outlines included in the organization's **annual work plan** are an integral part of its **annual exercise plan** and should therefore be created as part of the construction of this plan.

This will not only allow trainees to prepare in advance for each and every exercise; it will also provide them with anchors throughout the business year, which they can use to test their skills and readiness for possible real events. Therefore, the organizational exercise unit should construct the annual exercise plan in a way that most faithfully reflects the competency and readiness goals of the organization's management for that business year.

In creating the annual plan, the time constraints for the preparation of the various exercise types should be taken into account. A theoretical exercise usually requires a preparation period of one to two months. A functional exercise typically requires three to five months.

Another matter to consider when determining the mix of theoretical and practical exercises throughout the year is the fact that theoretical practice may always serve as a basis for practical practice.

Outline Creation Process

The outline creation process includes the following tasks:

01

Determining the learning objectives of the exercise (goal, the trainees' composition, subgoals, and practice topics).

02

Determining the practice setting.

03

Determining the timeline according to which the administrative division and trainees will prepare for the exercise (including setting dates for milestones on which the process is built).

04

Determining the necessary resources for planning and conducting the exercise (budget, manpower, physical location, technological and logistical means, etc.). Raising these resources in practice is the permanent responsibility of the organizational exercise unit, and handling it should, therefore, be scheduled as part of its overall work plan.

Determination of the Exercise Goal

The creation of the exercise outline begins with determining the goal of the exercise. The goal should be worded in terms that directly relate to the organizational cyberspace, and more precisely to the vision of improving and promoting the cyberresilience of the organization. However, the organizational cyberspace does not stand alone. Therefore, as a rule, it is necessary to also address continuity of the organizational function and business continuity.

An exception may apply in the case of an exercise at the techno-tactical level (such as one intended for low-level technological and operational factors in charge of the organization's cyberprotection). Goal setting should be based on all the relevant information accumulated in the organization up to that point, including lessons learned from previous exercises.

The following are typical and common goals that it is recommended to set for a cybersecurity exercise:

01

Raising management's awareness of the importance of cyberprotection.

02

Raising the awareness of employees in the organization of the importance of cyberprotection.

03

Exposing gaps in organizational cyberresilience (e.g., weaknesses and vulnerabilities in the architecture of the organization's ICT systems; its dependence on supply chains; cyberdefense processes fixed or practiced in it; the effectiveness and efficiency of its existing technical protection mechanisms, etc.).

04

Exposing gaps in the competence and readiness of personnel responsible for the organization's cyberprotection.

05

Exposing gaps in the competence and readiness of other components in the organization (individual functionaries as well as organizational frameworks).

At its formulation stage, the goal indicates the level at which the exercise will be conducted (strategic, operational, or techno-tactical), and hence the composition of the trainees. In fact, goals (1) and (2) presented above determine in their wording the composition of the trainees. Both are aimed at exercises at the strategic level.

Goal (3) above is aimed at the operational level but can also be aimed at the tactical level. In the first case, the administrative division perspective will be systemic, and hence most of the trainees will be senior- and junior-level executives responsible for carrying out the cyberprotection processes in the organization. The second case is the practice of selected components from within the organization, or even of a single component. Hence, the trainees will be both managers and employees concerned.

Goals (4) and (5) are tactical, or techno-tactical; therefore, the trainees in these cases will mainly be employees in different areas of expertise, with their area of expertise being much more important than their level of seniority.

It is highly advisable to focus on the practice of a single organizational level. It may seem sensible to use the exercise to address a number of goals, or, at the very least, to practice more than one organizational level, mainly for reasons of efficiency and resource saving. However, doing so will most likely undermine the effectiveness of the exercise. This is because the operation of each organizational level has its own unique internal logic.

It is not only that strategic interests are different from tactical ones; at times, they may even contradict each other.

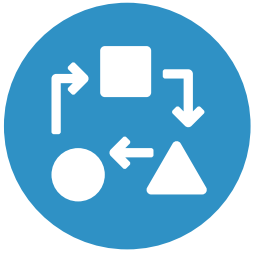
And since each organizational level sees a duty to itself to advance specific interests, the practice of each level creates a separate exercise. There may also be conflicts of interest among organizational levels. This does not require training the other levels; it is enough that they are simulated by the exercise administrative division through appropriate agents.

Determining the Practice Setting

Once the goal of the exercise and the trainee composition have been determined, the subgoals and topics of the practice can be determined. The next milestone in the creation process of the outline is the transition from the "what" (i.e., "What is the purpose of the exercise?") To the "how" (i.e., "How will this purpose be realized?"). The most appropriate setting for the practice in light of goal (1) above is a **tabletop exercise** (or an **organizational game**). In contrast, the most appropriate setting for goals (2) and (4) is an operational exercise. Goal (3) is, by definition, quite broad, and therefore the subgoals and practice topics derived from it must be defined as precisely as possible to select the most appropriate practice setting for its realization.

In general, if the realization of the exercise goal would require a broad systemic operation of the organization, it would be advisable to conduct an operational exercise; if the practice focuses only on certain components of the pan-organizational activity, then it would be advisable to conduct a **tabletop exercise** or an **organizational game**.

The practice setting to be constructed according to the outline may take many concrete forms. Practice settings, as defined in this guide (especially the tabletop exercise and the organizational game), are more like primary representative types, each of which may take a variety of forms. The decisive factors that influence the design of the practice setting for the exercise are those unique characteristics of the organization that have a bearing on the goal of the exercise, and the location and positioning of each trainee within the organizational structure. Box A1.1 is a representative case to illustrate the above.



Box A1.1. Company X Tabletop Exercise Schedule

Company X, which belongs to the chemical industry, owns a number of manufacturing plants that consume—and also produce—hazardous substances. In light of this, it has established a plan for preparing for crisis situations and dealing with them, whether imminent or already in progress. The plan encompasses the company's senior management and its plants. Following a comprehensive review of the plan, substantial changes were made to it. The senior management decided to examine the extent of the plan's effectiveness and the implications of adopting the changes in practice. To this end, the company's exercise unit built an exercise for its senior management and for the managements of all of its manufacturing plants. It was understood that it was appropriate for the exercise to be theoretical, and accordingly, it was determined that the exercise would be conducted in a tabletop setting. Considering the organizational structure of the company, the trainees were divided into teams by their affiliation (plants, senior management), and the course of the exercise was constructed as described in the table.

As can be seen, the exercise unit chose to implement the tabletop exercise by creating teams with representatives from each of the management groups in the company. Each team was given the opportunity to come together to deal with the developments of the scenario. In addition, the exercise unit established rules that regulate the exchange of information between the teams and themselves during the work in the team forum.

A framework was established that allows for cross-section reports at the level of the entire company.

Even though the way in which the exercise setting was designed did not change it from tabletop to operational, it nevertheless gave the exercise a more dynamic character, which made it closer, to some extent, to real-life situations. All this without departing from the general framework of a tabletop practice setting, as evidenced by the overall duration of the exercise, the quantity and composition of the trainees, and the relatively intimate nature of the event as a whole.

Time	Event	Location
09:00–09:30	Plenary Assembly: Opening, general briefing, and first news items release	Plenary Hall
09:30–10:15	Teamwork: Second news items release, teams split	Team rooms
10:15–11:15	Plenary Assembly: Cross-section report, free discussion, and third news items release	Plenary Hall
11:15–12:00	Teamwork: Fourth news items release, teams split	Team rooms
12:00–13:00	Plenary Assembly: Cross-section report, free discussion, and exercise summary	Plenary Hall
13:00–14:00	Hot wash	Plenary Hall

Approval of the Exercise Outline and Its Publication

Upon completion of the exercise outline (which includes preparation of the exercise indicator), it must be approved by the appropriate position in charge. In general, the organizational level of the certifying body should be one above that of the most senior trainee, or at the same level when that is not possible. This action is intended to obtain the backing and support of the position in charge of the exercise, to coordinate expectations as to the purpose of the exercise, and to make it a partner in the overall effort invested in preparing and conducting the exercise.

Once the outline has been approved, it should be officially published to bring it to the attention of the organization's management, the trainees, and any other factor involved in preparing and conducting the exercise. In doing so, ensure that the information published does not include details that are supposed to be hidden from the trainees. This refers, in particular, to the exercise news file. Also, do not include the background story of the exercise in the publication (if one was prepared). The background story should be distributed to trainees about a week before the date of the exercise.

Re-publication of the Exercise Outline

The exercise outlines included in the organization's annual business plan are published for the organization's employees as part of the publication of its overall business plan near the beginning of the business year in question. However, about a month before each exercise, the exercise administrative division must disseminate its specific outline to the trainees and to any other relevant factor to ensure that all are aware of the impending exercise and thus will be able to start to properly prepare for it. Even though the outline was prepared prior to the start of the business year, this point in time provides an opportunity for the organization to re-evaluate it and ensure that it faithfully represents the organization's expectations from the exercise.

Appendix 2. Guidelines for Creating a Cybersecurity Exercise Scenario

Overview

The activity described in Appendix 1 takes place prior to the opening of a new business year for the organization and is performed by its exercise unit. In contrast, the activities described below all occur before the beginning of each exercise. They are performed by the exercise administrative division, a temporary and dedicated body established ad hoc based on the permanent structure of the organizational exercise unit.

The Exercise Scenario's Construction Mechanism

Trainees act as **functionaries** performing **ad hoc tasks** derived from the practice topics to achieve necessary goals to advance the **organization's mission**. This dynamic is implemented through the work processes defined by the organization for this purpose.

The attacks included in the scenario aim **to challenge** this dynamic by methodically damaging weak spots that are present in the relevant organizational work processes. Behind these weak spots are the organization's cyberassets such as, for example, a computer controller installed in the organization's production infrastructure, or a software component installed in its IT infrastructure, each of which has some sort of vulnerability.

It is recommended that these vulnerabilities be known, or be similar to ones that are known, in cyberspace.[36] This will increase the scenario's credibility in the eyes of the trainees. In any case, the vulnerabilities should be reasonable, and the scenario should be realistic, plausible, and challenging. There is no impediment to including in the scenario a cyberattack that the organization has assessed as having a low probability of occurring but a high potential for damage.

Moreover, there is no impediment to using a cyberattack that, at least according to the major publications, has not yet been identified as a known threat.[37]

36. The weak spots were identified in advance and were selected as the focus of an exercise interest when setting the exercise subgoals and topics. They are not necessarily vulnerabilities built in to the hardware or software, but rather that result from poor settings or management of the organization's cyberassets (such as, for example, poor permissions for users in the organization or poor configuration of cyberprotection measures installed in the organization).

37. In this context it is worth mentioning the term "black swan" (defined by Nassim Taleb). This is a rare phenomenon that has a great effect and that seemingly cannot be predicted but is estimated to occur at some point. There is no impediment to including a black swan in the scenario, as long as it is convincingly incorporated into the overall web of events.

All that is required of the administrative division is to provide a proper logical basis for the initiation and execution of such an attack (i.e., the intentions and capabilities of an attacker and the feasibility of realizing the vector of the attack). After all, this is meant to be an exercise and not an experiment or a technological discussion.

Because it is a cybersecurity exercise, the organizational processes involved are based on the organization's ICT infrastructure or on the ICT infrastructure that connects the organization being trained to other organizations in its supply chain. Thus, the attacker's actions should strike, or threaten to strike, specific components of these infrastructures. In reality, these strikes are supposed to cause some damage to these processes in the form of disruption or shutdown. These, in turn, are supposed to cause operational damage to the organization.

The logical progression described above is applied, in effect, in reverse order as the exercise administrative division constructs each exercise cyberattack, just as a cyberattacker plans a real attack they intend to perform.[38]

Therefore, it follows that the first step in the process of planning the exercise attack is to determine the operational damage that will be caused to the organization. The administrative division of the exercise must first shape the process of **deterioration of the pan-organizational operational picture** in the exercise.

This will serve as the starting point for constructing any cyberattack that will be included in the scenario. But no less important, it will help the administrative division play out the **cybersecurity crisis** that the organization will fall into as a result of what is happening in the scenario. There are two types of cybersecurity crisis. The differences between them lie both in the way they occur on the timeline and the way the organization's understanding of what actually happens is evolving:[39]

38. In terms of its logic, the process of constructing an attack is based on the well-known and accepted models of cyberattack (such as, for example, the Kill Chain of Lockheed Martin, which appears in the Iceberg Model discussed in the main part of this guide).

39. This is commonly referred to as "situational understanding." In fact, the situational understanding of all trainees, and especially of those who are members of the organization's management, is one of the main issues to investigate following the exercise, since it attests to their ability to manage a cybersecurity crisis (build a situation report that reflects reality, make informed decisions based on it, manage their implementation effectively and efficiently, criticize the result, and so forth).

01

The evolving type: At the beginning of the exercise, no signs of operational or business damage to the organization are seen yet (i.e., on the surface, it is business as usual). At the same time, there are signs that may indicate, at the very least, hostile activity that threatens the organizational cyberspace. From there, the general situation is deteriorating, and cyberattacks against the organization are already beginning to take place. As a result, tangible operational or business damages to the organization are also beginning to occur.[40]

02

The sudden type: Cyberattacks start to occur at the beginning of the exercise (although the trainees may not yet have diagnosed it), and these attacks cause tangible operational or business damage to the organization. From this point, the general situation continues to worsen.

40. A special case of an evolving crisis is one in which no actual cyberattacks take place until the end of the exercise. Its use is mainly suitable for theoretical practice, and especially for an organizational game setting.

Organizational Weak Spots and Their Attack

The process described above ends with the determination of the weak spots in the organizational cyberspace toward which the cyberattacks included in the scenario will be directed. The following are typical weak spots:

01

A cyberasset that is common in the organization.

02

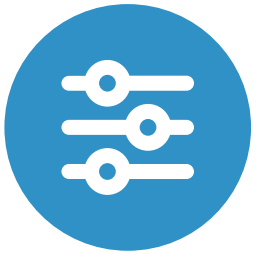
A cyberasset that is a single point of failure (SPOF).

03

A cyberasset that is an essential link in a value chain that supports one of the organizational processes that has been determined to be damaged within the scenario.

04

A cyberasset that supports the organization's supply chain.



The next step is to match the attacks to the vulnerabilities in the selected cyberassets. For reasons concerning both the credibility of the scenario and the administrative division's control during the exercise, the total number of attacks in the scenario should be between one and five. At the same time, the attacks should be constructed in an outline that will allow them to branch out during the exercise and even connect with each other. The product received will be a **complex** scenario (as opposed to a **packed** scenario).

A complex scenario will present trainees with a significant challenge to accurately interpret the signs that will appear in the exercise news items, in order to build a situation report that will faithfully reflect the reality of the exercise.

An equally significant challenge they will face is the operational management of dealing with the attacks. Even when the situation report is correct and complete, the situation itself is expected to present trainees with dilemmas as to the right course of action.

In other words, a complex scenario will challenge trainees on two levels of organizational activity: maintaining and preserving the continuity of critical organizational processes, while maintaining and preserving a cyberspace free of attacks, enabling and supporting both of these levels.

Exercise Noise

To ensure the credibility of the scenario and the effectiveness of the exercise, the cyberattacks in the exercise must be combined with "noise events," which is any occurrence in, or in the context of, the organizational cyberspace that is not a cyberattack or its consequence. These include technical and operational faults, as well as incorrect indications of various indicators (mainly in infrastructure and production systems, but also in infrastructure and IT systems).

Noise events must be credible, taken from the content world and the operative atmosphere of the trainees.

Beyond that, it is important that the signs alerting trainees to noise events be similar or even identical to the signs indicating the cyberattacks included in the scenario. Finally, even though they are the "chaff," while the cyberattacks are the "wheat," it is important to build noise events in a way that motivates trainees to act as if they were real attacks. Doing so will help to challenge the trainees both in analyzing the signs (in a form of triage) and in building the exercise situation report, as well as in managing their operational response in light of the state of affairs. At the same time, keep in mind that noise events have no value of their own. Therefore, make sure that their dosage in the scenario is not excessive.

To conclude this discussion, Box A2.1 offers an example of a noise event in the world of IT systems, which replicates the built-in tension between the operational level and the ICT level in the organization.

Box A2.1. Example: Noise Events

As part of the practice of a large retail chain, the administrative division built a noise event in which, while updating the price of a particular product, the digit "0" was inadvertently entered in the network database instead of another digit. The product in question is sold only in some branches of the chain, and accordingly this update has been distributed only to them. As a result, the points of sale in only these branches collapsed due to a division by 0 performed by a certain algorithm in their operating system.

At the time of distribution of the exercise news items related to this event in the exercise, the network was already also subject to exercise cyberattacks, and the trainees were well aware of this. Now they were faced with a dilemma: should they assume that this is another cyberattack, and accordingly perhaps voluntarily disable, for example, the sales terminals in the other branches of the chain, or take the risk of assuming that it was a malfunction and let the sales terminals in the other branches continue to operate properly?

Cyberattack vs. Cybersecurity Event: Deriving the Exercise News Items from the Exercise Scenario

The long heading above is intended to differentiate between the angle from which the administrative division sees the details of the scenario, and that from which the trainees see them. As the body that constructed the scenario, the administrative division knows why and how everything happened in it. The trainees, on the other hand, see only the exercise news items, which represent only the visible effects of the chain of events that the administrative division has constructed. Thus, for example, while the administrative division knows that one such development is, in fact, a noise event (rather than a cyberattack), trainees may interpret its signs as if it were a cybersecurity event.

The difference between these two perspectives is an essential feature of the practice, and it reflects, in its own way, the built-in difference between the attacker's vision and the defender's vision. In light of this, when deriving an exercise news item from the scenario, it is extremely important to make sure that the information transmitted in it does indeed reflect in the best way what the trainees would be expected to know if such events happened in reality. Box A2.2 offers an example to illustrate this point.

As can be seen from the example, the news collection in question cannot in itself indicate that the source of the problem created is a cyberattack against the digital payment system. Trainees have a responsibility to investigate what is happening themselves to find out. Of course, the dynamics described here were developed by the administrative division to motivate the trainees to act in a certain way, while preserving the realistic and authentic nature of the occurrence.

Deriving the exercise news from the scenario is the first of two steps in realizing the simulation component in the exercise. This step is performed before performing the exercise. The second step—managing the process of delivering the news to the trainees—takes place during the exercise itself. In fact, it is the core of the administrative division's occupation in this framework.

Box A2.2. Example: Deriving Practical Knowledge from the Exercise Scenario

As part of a practice of the overland public transportation system, in which the relevant government agencies also participated, the administrative division built a cyberattack on the digital payment infrastructure that supports it. As a result, clearing systems on buses and on train stations ceased to detect the digital means of payment held by passengers, which, of course, led to serious disruptions in the functioning of public transportation.

In order to build on the exercise news items derived from this attack, the administrative division examined the progression of this event: the bus drivers and the workers at the train stations will, obviously, be the first to notice the abnormal occurrence. At the same time, the passengers are expected to show great resentment over what is happening, and in the current era, this will soon widely echo on social networks. From there, it will very quickly reach the mass media as well.

At the same time, it is likely that this resentment will lead to various manifestations of violation of public order, so that the police will also be involved. This derivation process, based on the simple logic of "one thing leads to another," led the administrative division to create news items containing appropriate reports from drivers to the bus companies' operations centers, parallel news for train infrastructure, and media reports reporting the above disruption, as well as the disturbances and uproar spreading among the general public.

On top of that, the administrative division added a news item with a police request to government officials regarding clarification of the details of the event and how to proceed in treating it.

Appendix 3. Guidelines for Conducting a Cybersecurity Tabletop Exercise and a Cybersecurity Organizational Game

Overview

The difference between the theoretical and the practical practice methods is noticeable in the difference between the actual modes of conducting exercises performed according to these two methods. Thus, this appendix will deal with conducting a tabletop exercise and an organizational game, and Appendix 4 will deal with conducting an operational exercise. Although the items presented below are aimed at the practical level, the understandable limitations of the breadth of this guide require focusing only on key points, and should not be seen as a recipe that can be applied directly and habitually.

General Time Frame

The total length of a tabletop exercise should not exceed half a day (usually, a period of one and a half to three hours is sufficient). It is also advisable to conduct it in the first part of the day.

Practice Environment

In its classic configuration, a tabletop exercise is held around a single table. This means that trainees sit at this table, and it is important to ensure that everyone can see each other. Hence, it is common to call an exercise of this kind a "roundtable." But the table does not have to be round, and in any case, it has an "end point," or a head: this is a seat designated for the **exercise moderator**.

In practice, due to the limitations involved in the physical performance of the exercise, there may be a situation where there will not be enough space around the table for all trainees. This happens when at least some of the practiced functions are represented not by a single functionary, but by a team of several functionaries. In such a case, an outer circle of seats (the "second circle") can be placed outside the table and the seats arranged directly around it (the "first circle").

Then, the functionary who is most senior (or central, in terms of exercise goals and topics) on each team will be the one sitting in the first circle, and everyone else will be positioned in the second circle, behind them and next to them. The second circle is also meant to be used by the members of the exercise administrative division (it is customary for its head to sit in the first circle), including agents and lookouts.

It should be emphasized that the exercise discussion should take place, at least for the most part, among the occupants of the first circle. Therefore, in order to ensure the effectiveness and efficiency of the discussion at the table, it is important to make sure that the total number of people sitting in the first circle is, **at most, between 20 and 30**. The total number of trainees may, however, be higher, and for this reason it will be necessary to adjust the size of the hall where the exercise is held to accommodate all the participants.

As mentioned before, the conducting of a tabletop exercise is characterized, as a general rule, by the units of time (the designated time frame) and space (the practice environment). Thus, this practice setting is particularly appropriate for any situation where, for example, considerations of information exposure permissions, or dictates arising from the organizational structure of the company and how its departments are divided, that may require internal partitioning of trainees from one another are not present. Alternatively, the goals of the exercise may be such that in order to achieve them, the creators of the exercise will choose to drop down such partitions intentionally.

However, it is sometimes right and necessary to compartmentalize the trainees for the purpose of conducting the practice. The typical and common case is that of an organizational game. Under such circumstances, the practice cannot be held in one common space. The trainees are divided into teams, each of which is located in a separate room or hall (or at a proper distance from the other teams).

Where any such team operates under conditions of unity of time and space, all that has been written above in this regard applies. Moreover, even in an organizational game it will probably be necessary to occasionally gather all the trainees together in one space (plenum).

The plenary assembly is mainly used for the purpose of performing a cross-section report, which allows trainees and the administrative division to understand the overall exercise situation. The summary of the organizational game and its hot wash will also be carried out in the plenum.

Managing the Exercise

The exercise moderator sits at one end of the table. Their role is to conduct the exercise discussion, while the administrative division rolls out the scenario by passing on the exercise news to the first-circle occupants, thus helping them achieve the goals of the exercise. The moderator may also be a trainee (and in such case, their true organizational role has clear managerial significance in the exercise). Alternatively, they may be a member of the administrative division, but usually not the head of it. As such, they may be an agent, but there may be cases where their role will be purely managerial (i.e., they will not play any role taken from the organization which has a direct and practical affinity to the exercise goals and topics). Therefore, the moderator should:

01

Have basic managerial experience, which includes the skill of moderating discussions.

02

Know the organization being trained.

03

Motivate the exercise discussion according to the goals and topics of the exercise and according to the exercise clock, while controlling the dynamics of the discussion.

04

Maintain a proper culture of discussion.

If the moderator is also a trainee, they are not exposed to the scenario, and the logic that drives their actions stems from the definition of their organizational responsibility and the way in which they are expected to implement it in light of the circumstances of the scenario. In this case, it is the responsibility of the administrative division to ensure at all times that the moderator's action serves its intended purpose. In contrast, if the moderator is a member of the administrative division, they should be familiar with the organizational processes and procedures involved in the exercise (methodically), and since they know the details of the scenario, they have less need for the administrative division's direction.

For the record, the head of the administrative division alone is authorized to make decisions regarding the timing of the practice (setting its actual commencing time, setting breaks or canceling them, accelerating or slowing down the scenario roll rate, and setting its end time).

In an organizational game, a moderator will be assigned to each team of trainees (besides an additional moderator for the plenum). In this case, it is typical and common for the moderator to be one of the team members, but this is not a hard and fast rule. Due to the greater managerial complexity that exists here, the administrative division should use its lookouts not only to regularly document team activities, but also to assist the administrative division in monitoring the activities of all teams and directing them in light of the exercise goals.

Technical and Logistical Preparation of the Practice Environment

In the main part of this guide, reference has already been made to this matter, which touched on the common technical and logistical aspects of theoretical and practical practice.

These aspects are unique to theoretical practice:

01

The preparation of the practice space must be completed a day before the date of the exercise.

02

It is advisable to place a pad or notebook and a pen on the exercise table for each occupant of the first circle. This will encourage them to bring up thoughts in writing, and will thus help to clarify the issues that emerge during the exercise. Furthermore, trainees' notes can assist them in carrying out the hot wash and the in-house debriefing that will follow. As a rule, a trainee's notes are their personal property, and they have the right of access to what is written in them. If a trainee chooses not to take their notes with them at the end of the exercise, the administrative division has the responsibility to destroy them.

03

On the day of the exercise, the documents containing information concerning the topics of the exercise (work processes, procedures, etc.) should be made available to the occupants of the first circle. Make sure to collect these documents at the end of the exercise and return them to their storage place in the organization.

04

Members of the first circle should be given name tags (full name, organizational affiliation, and job title). This will make it easier for them to position themselves around the table and identify each other.

05

In addition, it is important to register the participants at the beginning of the day. Each of them should be equipped with a personal ID tag. This will not only assist the administrative division in monitoring the composition of the participants, but also prevent entry into the practice space of factors who are not supposed to participate in the exercise.

Further to this, and certainly in cases where there are sensitive practice issues, there should be constant control of those entering the practice space until the end of the exercise.

06

There is great benefit in displaying the exercise news items on monitors installed in the exercise space. The benefit increases as the number of trainees increases. A printed copy of each news item should be given at least to the occupants of the first circle, so that they can sketch for themselves the development sequence of the scenario.

07

If the duration of the exercise does not exceed two hours, it is advisable to avoid taking any breaks, as this may impair the exercise tension and its dynamics. For a longer exercise, one break should be provided.

Appendix 4. Guidelines for Conducting a Cybersecurity Operational Exercise

General Time Frame

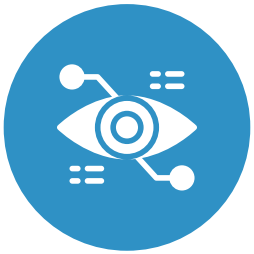
The length of an operational exercise may range from one day to several days. In general, it is directly proportional to both the scope of the factors and bodies being trained, and the level of organizational complexity of the exercise.

Practice Environment

It is important to reflect most of the components of the real environment in the practice environment. Beyond soft components such as methods of operation and procedures, these are, for example, also the means of communication that the organization uses in real time (and with an emphasis on crisis situations).

In operational practice at the techno-tactical level, the unity of the place is usually maintained. Even if it is a matter of several teams practicing in parallel, each located in a separate room or even building, these practice spaces will most likely be adjacent to each other. The effectiveness of this type of exercise depends crucially on the proper image of corporate cyberinfrastructures of different types (in the IT and OT worlds), as well as of different types of cyberattacks aimed at them.

Unsurprisingly, this is a professional and resource-intensive field of expertise, which requires dedicated infrastructure, resources, and manpower, and which usually actually takes the exercise out of the organization's physical space to various external facilities that provide such a service (indeed, there are quite a few in Israel and around the world).[41]



This characteristic distinguishes techno-tactical practice from that of other levels of the organization, since it involves meaningful logistical and economic considerations.[42] However, in this case the practical distance between exercise and training is quite small, so that the practice needs of the organization at this level can be involved in its training needs, and in this way save considerable resources.

When it comes to an operational exercise at the operational and strategic level of the organization, the unity of the place usually does not exist. Therefore, the trainees may be physically and even geographically located in different places. Thus, for example, in the case of an operational exercise of several manufacturing plants grouped under one company (whose management is also being trained), it is possible that the exercise will be conducted simultaneously at sites spread over a large area of the country.

Unlike theoretical practice, there is no pre-set limit on the number of trainees, and the only limiting condition is the administrative division's ability to control the course of the exercise, and, in the case of a techno-tactical exercise, also the capacity of the simulation infrastructure supporting the practice.

Managing the Exercise

To exercise proper control over the process of an operational exercise at the operational and strategic level, the administrative division should first establish an **exercise control center** (hereinafter, **ECC**) through which the exercise will be conducted in practice. The administrative division will place lookouts in the practice spaces, who will serve as its eyes and ears.

The object of observation of the lookouts is the human function (of functionaries and teams) and not the function of systems and infrastructures—that is, verbal statements by functionaries in their day-to-day work and in various forums, and any additional information available, accessible on monitors or through written documents.

41. Operational exercises conducted in such facilities are usually similar in character to that of an organizational game, or more precisely, of a competition between teams. A well-known example of this is NATO's Locked Shields exercise, held once a year at its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia.

42. While intra-organizational capability can be developed in this field, in view of the costs involved in development, day-to-day use, and long-term maintenance, as opposed to those involving outsourcing, it is clear that this effort is worthwhile and profitable only for particularly large organizations (and, not surprisingly, government organizations such as various security agencies).

The lookouts will be in constant contact with the ECC, and the administrative division will use their reports to assess the condition of the exercise. This should be done as a default at least twice a day (shortly after the beginning of the practice day and towards its end), as well as whenever it appears that the pace and direction of the practice is not in line with the plan.

As a rule, it would be right to place the lookout assigned to monitor the activity of a particular practice space in the nerve center that dominates the activity of that space. (For example, in the example of the production company practice presented in Appendix 1, it would be right to place the organization's chief executive lookout on the site where management conducts its status assessments. The same applies to the lookouts who will be stationed in the company's factories. It is also possible that the administrative division will place lookouts in positions of control over the production infrastructure of the factories.)

Due to the physical dispersal of the trainees, and also for the purpose of supporting the control of the exercise process, the exercise news items should be delivered in a computerized form.[43] In light of the above, and assuming that the organization does not have a dedicated ICT infrastructure for this purpose, it would be best to use the message system that will serve the communication among the trainees and between them and the administrative division during the exercise for that purpose.

Just make sure that the infrastructure in question allows the delivery of both written messages and audio and video files. Dedicated user accounts for all trainees should be set up for the exercise in the selected system, which will be used both by trainees to communicate among themselves during the exercise and by the administrative division to deliver the exercise news items to them.

The administrative division may perform an action known as a practice methodical stop during the exercise. This stops the process of delivering news to the trainees for a defined period of time, and as a direct result freezes the development process of the scenario for this period of time. This action allows trainees to perform a situation assessment free from time constraints and the new challenges that the scenario is designed to have them face.

43. The use of mechanized means of communication will make it possible to reliably, conveniently, and easily document the information that "flowed" during the exercise between the administrative division and the trainees and among the trainees, and thus, the resulting information base will serve as a top-notch source of information for investigating the exercise.

The administrative division may also choose not to deliver a series of exercise news items to the trainees, either because a particular exercise subgoal has already been achieved, or to proactively and artificially promote the unfolding of the exercise scenario after it has progressed at a slower pace than planned.

Technical and Logistical Preparation of the Practice Environment

The following are the aspects unique to an operational exercise at the operational and strategic level with respect to technical and logistical preparation of the practice environment:

01

As in the case of theoretical practice, so in practical practice the administrative division's main technical and logistical effort is to establish and preparate one site, the ECC. Unlike theoretical practice, in practical practice trainees must invest their own preparation efforts to establish their practice environment. This is to stress that this responsibility lies with the trainees, not with the administrative division.

02

Determining the location of the ECC and planning its functional organization and physical preparation are done as part of the administrative division's overall preparation process for the exercise. They must be completed at a time that will allow the ECC to reach full functional capacity no later than two days before the exercise.

03

As in a tabletop exercise and an organizational game, so in an operational exercise, participants must register when the exercise opens (this is true for all practice areas, including the ECC), and controlling those entering the practice areas must continue until the end of the exercise. Here, too, each participant must be equipped with a personal ID tag.

04

Unlike theoretical practice, in practical practice there is almost no reason to have the administrative division stop the practice, since to the extent possible each of the trainees functions in this framework similarly to the way they operate in reality.

Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered.

Organizational readiness is dynamic, and therefore it should be examined from time to time. One of the main tools available to the organization for this purpose is exercising, designed to promote the competence and readiness of the individuals of an organization through qualities that require gradual construction, ongoing maintenance, and promotion according to a plan.

As in other arenas, conducting exercises in the cyberworld is an important key to preserving and promoting the resilience of the organization. This initial and unique guide is intended to be used by economic organizations as a basic tool for creating cybersecurity exercises, conducting them, and drawing conclusions in an orderly fashion.

Nitzan Amar
Senior Head of Division, Resilient Infrastructure

Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered. The list of documents presented below reflects the state of the collection at the time of publication of this document.

Volume A: A methodological approach

- **A.01** Cyberdefense Methodology for an Organization 1.0
- **A.02** Cyberdefense Doctrine 2.0
- **A.03** Use of Cloud Services: Addendum to the Organizational Cybersecurity Methodology
- **A.04** Organizational Coping in Cyberspace: The Insider Threat
- **A.05** Organizational Preparedness for a Cybercrisis
- **A.06** Supply Chain
- **A.07** Focus Questions for Cybersecurity Policymakers
- **A.08** Recommendations for Information Security and Reduction of Cyberrisks for Small Businesses
- **A.09** Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization
- **A.10** Cyberrisk Management in the Operational Technology (OT) Environment
- **A.11** Risk Assessment Template: Retail Sector
- **A.12** Cyberpractice: How to Plan a Cybersecurity Awareness Program

Volume B: A technical approach

Volume C: Secure software development