NÚKIB

National Cyber
and Information
Security Agency
of the Czech Republic

HOW TO DEVELOP A CYBER SECURITY TABLE-TOP EXERCISE

A PRACTICAL GUIDE

www.nukib.cz

CONTENT

PREFACE

How can governments and other entities involved in enhancing cyber security stay ahead of evolving threats represented by cyber-savvy criminals and hackers? Staying up to date on technology developments, and being able to quickly adapt to new threats, requires being cyber-aware. This may be ensured only through continuous learning processes. Dedicated lectures, courses, seminars, reading books – all are useful and favored. However, one more method of education exists and is specific for several reasons – cyber security exercises.

IT experts are usually not fully aware of the impact IT products and technology solutions may have on national security and technical personnel on the operational level is often not familiar with the processes of political, diplomatic and strategic decision-making. Likewise, senior leadership, law enforcement officials and policymakers face difficult challenges in their work without necessarily knowing the technical implications and impacts associated with cyber incidents. Cyber exercises pose a great opportunity for how to get technically skilled professionals and government representatives in conversation, to confront each other with their different perspectives on problem solving. In addition, cyber exercises enable stakeholders to tackle important aspects of responding to incidents – such as the deployment of technical solutions, teamwork, information sharing or cooperation – in a safe and secure environment. It can provide real-time evaluations or lessons learned, which is especially important for reviewing and improving internal procedures, contingency planning, crisis management etc. Aside from the knowledge gap between technical staff and decision-makers, varying capabilities and skills between younger and older generations must also be taken into account. Given the practicality, interactivity, and not least given the fun element, which exercises usually offer, these might be the appropriate form of education for every age group. Thus, effectively targeted and crafted cyber exercises can contribute to the digital literacy of a population. The more cyber-knowledgeable the population is, the more digitally-secure the country becomes.

INTRODUCTION

CONTEXT

Crisis/full-scale management exercises and military exercises are among the pillars in ensuring security. They have been conducted for many years as a means to train readiness for military operations and emergency management procedures in cases of natural disasters. The merit (and success) of these exercises lies in their ability to adapt to real environments/reality. Given the increase in recent years in the importance of IT dependencies, hybrid threats involving cyber warfare, and the proliferation of IT technology within the daily lives of citizens, businesses, and governments alike, cyber security and cyber defense have received more attention in the education and exercise area. Consequently, many institutions and businesses participate in cyber exercises that are increasingly recognized as the perfect learning tool.

PURPOSE

The purpose of this handbook is to provide context and guidance for planning, developing, organizing and improving cyber security table-top exercises. It has been written not only to introduce the topic, but also to give practical advice on how to plan, design, run, and evaluate exercises. It is however neither a detailed step-by-step plan nor a technical guide.

AUDIENCE

This handbook is intended for those responsible for protecting and operating critical information infrastructure, important information systems, or any kind of high-value assets. The primary goal is to help the less experienced to carry out their own exercises by showing how these can be developed, and to help those who are already conducting exercises to get the best possible results. The handbook also serves as a reference framework to compare possible approaches of conducting exercises.

SCOPE

The handbook describes how cyber exercises might be designed, in order to effectively educate and train different target groups, ranging from technical personnel to executives and political leaders. Based on the experience of the Czech Republic since 2014, when the first national cyber security table-top exercise was held, the handbook offers a framework and methodology for designing exercises. In addition, it integrates key lessons learned and recommends best practices.

CHAPTER 1
EXERCISE TYPOLOGY AND DESIGN

EXERCISE TYPOLOGY

Cyber security exercises can be divided into a number of types: table-top, technical, communication, simulation, war gaming, capture the flag, procedural or hybrid. These share some overlaps between each other. The geographical distribution of participants may pose another dividing criterion. We may distinguish national, bilateral, regional, international or even global exercises. Regardless of the type, all exercises enable participants to tackle important aspects of responding to security incidents, such as teamwork, information sharing and institutional/cross-border cooperation etc.

While technical exercises are designed to practice primarily technical skills and capabilities, discussion-based exercises are often used for testing procedures, crisis management processes and institutional arrangements and agreements. Non-technical exercises are moreover helpful in creating new or reviewing old continuity plans and policies. They may also serve new staff and not fully cyber-knowledgeable leadership as orientation to the field.

Exercises aimed at practicing decision-making processes and procedures can be conducted as *non-technical/table-top exercises (TTX)*. There is no need to use virtual environments to expose senior leaders to cyber-related matters. All that is needed is a relevant scenario and injects tailored to the given audience. The scenario should engage decision-makers to take effective decisions and relay orders to lower echelons. Executives might not be IT-knowledgeable, nor might they have to face cyber-related challenges on a daily basis. Accordingly, they may not be capable of adequately assessing a particular crisis. A TTX is one of the best tools to educate decision-makers on the importance of cyber security and its relevance to national security. According to the tools you involve in the exercise, TTXs can be further divided as rudimentary (only paper and pen needed) or more advanced (more „sophisticated“ tools involved, e.g. digital platforms, applications for online editing and sharing documents, exercise news portal, audio-visual tools etc.). From the exercise objective perspective, both hold high value.

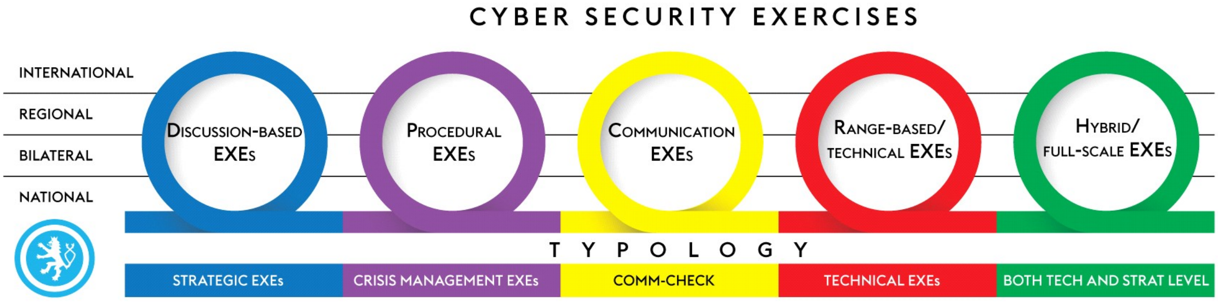


Figure 1: Cyber exercise typology including a geographical aspect.

Unlike TTXs, *technical exercises* planned and executed in cyber ranges allow for testing individual and collective technical skills while responding to cyber-attacks. Therefore, they are more suitable for experts with IT knowledge and experience in system administration and securing infrastructure. Such range-based exercises expose those IT professionals and administrators to the imperatives of configuring, setting up, installing, and practically securing dedicated infrastructure, as well as investigating, analyzing, and handling complex cyber incidents. One of the best and most used hands-on concept of technical exercises is the *Red team/Blue team* model.[1] A Red/Blue team exercise is based on a model within which exercise participants form Blue teams that are responsible for the protection of a dedicated infrastructure. Defending teams face real-time attacks (performed by the Red team) escalating from simple attacks (application denial-of-service, defacement,…) to the more advanced ones (exploits, specially crafted malware, logic bombs, etc). Alongside the technical aspect, blue teams have to react to company users' issues and complaints, and assess the potential legal and media impacts of the incidents. The range of training objectives is usually wide and covers the practice of technical skills, work in increased stress situations, and the communication aspect. Blue teams are scored for maintaining usable environments for end-users, for availability, information sharing, communication with media and legal advisors. Awarding points should promote healthy competition and provoke better performance through gamification.

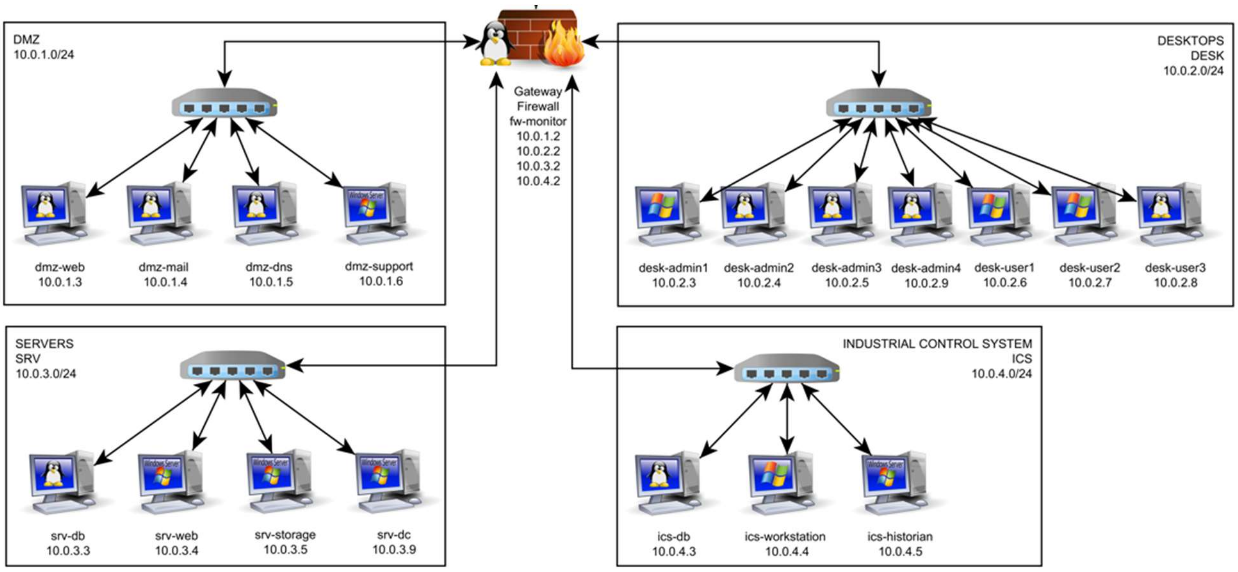


Figure 2: An example of the technical infrastructure during the Cyber Czech 2016 exercise. The infrastructure consists of 4 network segments (DMZ, Clients, Servers, ICS) and a central firewall.

Communication exercises are extremely important for testing the availability of points of contact (PoCs) in given institutions, and for testing whether and to what extent the points of contact are up-to-date. We would not strictly classify them as either technical or non-technical. A major goal of these communication exercises, (sometimes also called "comm-checks") is to regularly verify availability and how much time it takes to reach out to an institution/person relevant to solving a potential incident or crisis.

Hybrid exercises can be viewed from a variety of perspectives. For the purpose of this guide, a hybrid exercise is considered an overlying and interconnecting concept of the abovementioned exercises. In this sense, a hybrid exercise combines a technical exercise with a strategic level TTX, allowing participants from the technical layer of cyber security to train together with the highest-level decision making entities in one exercise. As such, it offers an "all-inclusive" package for players to train both technical and decision making

[1] Technical exercises may also include hackathons, capture the flag, competitions etc.

capabilities, via interaction between these two specific levels. Nowadays it is not possible to strictly separate the technical world from the political or strategic.

Since this is a rather advanced model of exercise, it is worth deploying it only after you have gained enough experience with technical and table-top exercises. Hybrid exercises can realistically only accomplish positive outcomes when they are properly prepared, and when the operational level (and the sum of its outcomes) is logically linked to a strategic intent, and vice versa. This might be very challenging, especially when linear development on the technical layer does not correspond to the time-based nonlinear aspects of decision making at the strategic level. Unlike cyber-attacks, decision making - often burdened by bureaucracy - might seem to be too slow.

The cyber defense exercise Locked Shields, organized by NATO CCD COE, might serve as a good inspiration and example of a hybrid exercise ([https://ccdcoe.org/locked-shields-2017.html)](https://ccdcoe.org/locked-shields-2017.html).

Note: Hybrid exercises should not be confused with the concept of hybrid as the nature of a threat (combining kinetic operations with irregular and cyber warfare).

The type and scope of an exercise should be selected based on available resources and exercise objectives to be achieved.

EXERCISE DESIGN

Design questions should be dealt with after the exercise type is outlined, in order to drive subsequent planning steps. Design decisions must go hand in hand with the basic objectives of the exercise. E.g.:

- *Do we want to test the IT security team's speed to recognize, analyze and respond to a cyber incident?*
- *Will the exercise test the roles of law enforcement, the intelligence community and military bodies, as well as their coordination and information exchange procedures during crisis?*

What else must be decided before we start planning?

Here are examples of questions worth addressing during the initial planning stage, in order to select the right exercise concept.

- *Will the exercise simulate reality by running 24/7, or will it be phased over a two-day/one-week period condensed into a very busy 6-hour exercise, where a few hours reflects some pre-determined time passage?*
- *Is the exercise aimed at practicing crisis management only during office hours, or conversely, does the exercise intend to test readiness outside of working hours, or even during the weekend?*
- *What other specific tasks, functions, roles, or activities does the exercise intend to evaluate?*
- *What are all the components that could be simulated in order to make the exercise authentic?*
- *What hardware or equipment does the exercise require – computers, phones, mock news reports or any other tools?*
- *Is an exercise team/unit present in your institution? What is the maturity level of that team? Do they have any experience with conducting the selected type of exercise? How much time do they need to get familiar with the preparation mechanism/exercise lifecycle?*

The optimal length of a table-top exercise is around 60-90 minutes (excluding break time).

It is important to note that the longer a training session is the more difficult is to keep trainees' attention. Thus, long duration can affect the overall outcome of the exercise.

Another option is to train various target groups and scenario escalations across different layers of decision-making. In that case, the exercise can take a day or even two, excluding time set aside for set up and evaluation. Attendees might be involved in only certain portions of the exercise, when the issues covered are most relevant to their agenda and level of competence. E.g. high-ranking officials will not be able to stay 8 hours at the exercise venue, especially without contact with the outside world. It is advisable to make policymaker participation effective by tailoring the exercise environment to their specific needs. Despite such customization, the goals of the exercise may still be met.

CHAPTER SUMMARY

- **According to your needs, capacities and resources, select the most suitable exercise design. In this step, always consider the exercise purpose and major goals.**
- **Tailor planning to the experience and skills of exercise designers.**
- **An exercise must be feasible in all aspects – funding, preparation time, human resources, facility, technology, leadership support and other resources.**
- **Remember, if real decision-makers participate, you will not get a second chance to make your point.**

CHAPTER 2
EXERCISE OBJECTIVES AND TRAINING AUDIENCE

EXERCISE OBJECTIVES

One of the first steps in the planning stage is to determine the purpose and intended objectives of the exercise. This must be logic-driven, based on the exercise design chosen in the previous step. Examples of core general exercise objectives might include to:

- practice technical skill;
- train coordination and complex response measures to cyber incidents;
- grasp the broader national security implications of a wide array of cyber incidents;
- practice communication and information sharing with counterparts (other CERT teams, media, private sector, law enforcement bodies etc.);
- practice reporting to managers and decision-makers;
- train teamwork (delegating, dividing and assigning roles);
- exercise time management and prioritization;
- expose and validate cyber security/defense policies and procedures;
- experience work under stress and time pressure;
- gain deeper understanding of the technical, political, strategic, diplomatic and legal contexts of cyber crises;
- improve the ability to convey the big picture;
- test a new organization, technology, tools, processes and thereby reveal weak spots and points of friction;
- enhance cyber education and awareness at all levels;
- and many others.

The number of objectives should be balanced to keep the exercise manageable. Objectives can be broken down into main goals and ones that are more specific. E.g. the main objective of a technical exercise might be to test technical capabilities, whereas the specific training goals may be defined as training incident handling processes, reporting to the higher echelons, analyzing specific malwares, conducting forensic investigation, writing technical analysis, practicing reverse engineering, and so forth.

All objectives should be measurable. In other words, they should be clearly defined, realistic, reasonable, and in accordance with the organization´s visions, principles, competencies and current and future challenges the organization faces. Where this serves a purpose, a time limit should be set to determine by when the tasks are to be completed.

TRAINING AUDIENCE

In order to solve incidents rapidly and properly, all relevant entities must be involved in working towards the solution. Cooperation and coordination across the security community (*horizontal perspective*) is a key and irreplaceable element in dealing with serious incidents. In this regard, exercises offer an excellent opportunity to establish or strengthen relationships and trust. Cyber-attacks (even if trivial on first sight) might escalate, and stakeholders from various fields might be affected as a consequence (as indicated in Figure 3). Inviting representatives from different spheres and sectors to the exercise event creates opportunities for effective future collaboration. Cooperation and information sharing is used in real life to help organizations better protect themselves against cyber-attacks; cyber exercises simulating those attacks should be treated the same way.

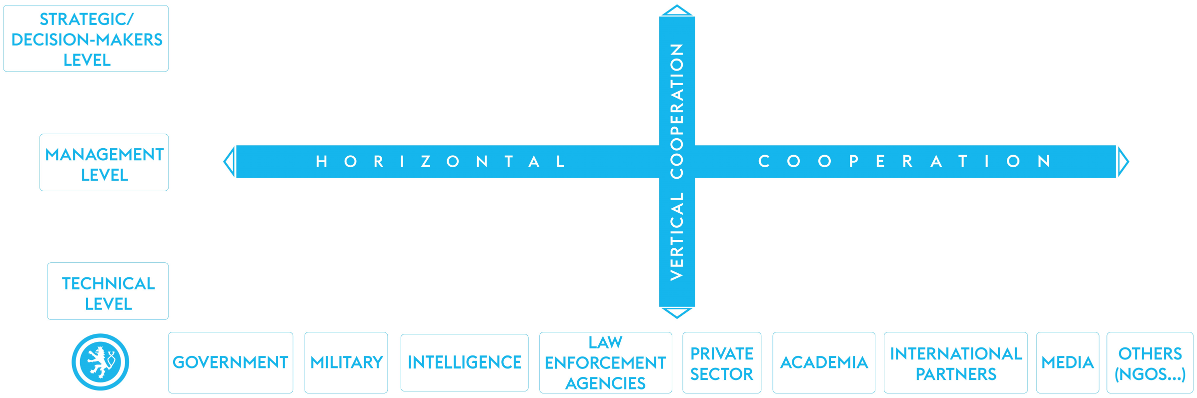


Figure 3: Illustration of the whole-of nation approach.

To demonstrate the point, the following is presented as an example of an incident which escalates and impacts various domains.

„Several regions across country X suffer power outages. These outages affect several major industrial areas and even a military base experiences a partial power outage. Due to unexpected technical difficulties, back-up generators are unable to begin providing the military facility with electricity directly after the blackout occurs. Best estimates suggest that recovery will take at least 10 hours. The current situation affects the everyday life of country X's population. The mood worsens as the blackout leaves millions of people without electricity. The outages induce public unrest, with protests in the streets. According to investigators, the loss of functionality was caused by a malware attack that might have been conducted by a group of attackers linked to a nation state."

Domains that might be affected by such an incident (*the following questions can also steer the process of formulating the exercise objectives*):

GOVERNMENT – The government faces a crisis with a national impact, due to the limited distribution of energy and outages.

- *What governmental department should be the lead in dealing with this situation to coordinate the responses of multiple governmental entities?*
- *Is there an option to legally and operationally prioritize electricity supply to critical services such as military and national security installations, healthcare systems and emergency services?*
- *Are necessary policies, personnel, and recovery plans in place for large scale cyberattacks that affect the whole population?*

MILITARY – Since there are partial electricity shortages at the military base, military capability is affected as well.

- *Would a cyberattack on the electricity grid be considered legitimate grounds for use of force it such an attack compromises the defensive capacities of the state? On what basis?*
- *Is the military legally and operationally able to conduct active defense operations in peacetime conditions (according to IHL)?*

INTELLIGENCE – To defend against such an attack, the role of cyber threat intelligence analysts is critical.

- *Is the malfunction considered an intended attack?*
- *Are the attackers linked to a nation state? How can the attack be attributed to the attackers?*
- *What else is known about the attackers and their motivation?*
- *Are tools in place to gain sufficient insight?*

LAW ENFORCEMENT ENTITIES, LEGAL ADVISORS – After the incident is detected, the investigation process begins.

- *Is there a legal framework in place to respond to a cyber crisis?*
- *Are the legal conditions for declaring a state of emergency fulfilled?*

PRIVATE SECTOR - The SCADA management systems of different private electricity distribution companies were attacked.

- *What information would be exchanged with affected private companies?*
- *Is there an established list of points of contact?*

INTERNATIONAL/DIPLOMATIC ASPECT – An attack on the electricity grid can damage the electricity grids in neighboring countries if they experience a large-scale overload and/or instability.

- *Are there means for contacting the neighboring state authorities to mitigate possible impacts of the disruption on their electricity grid?*
- *Are there funds available to compensate for any possible cross-border damages?*

MEDIA – Due to time pressures, media will usually begin reporting without a deeper understanding of the situation. Moreover, getting sufficient information from the affected area is problematic due to the blackout itself.

- *How can the government effectively communicate its position and recommendations to the citizens if these are out of electricity power?*
- *What will be the communicated narrative?*

PUBLIC – Disapproval with government response may move people to the streets. Public trust in government decreases dramatically.

- *What will be the communicated narrative towards the public?*

Depending on the objectives/specific objectives of the exercise, relevant entities on the horizontal line of Figure 3 must be represented in the exercise.

Additionally, the *vertical perspective* has to be taken into account. During exercise planning, all necessary levels of the "chain of command" must be assessed, so as not to omit any level important to the passing and carrying out of orders. Starting with a clear identification of primary exercise objectives could help better understand what level (operational, tactical, strategic, all?) the exercise should focus on. Let us go back to our possible scenario.

TECHNICAL/OPERATIONAL LEVEL – Since critical services and SCADA systems were compromised, the computer emergency response team (CERT) and technical/SCADA experts are included.

- *How quickly will they be able to assess the severity of the situation?*
- *How and through what channels will they report incidents to the higher echelons?*
- *Who will they ask for assistance?*
- *What information would they share with partners?*
- *Do they have the necessary tools/skills to analyze the malware?*

MANAGEMENT LEVEL – Management is responsible for assessing the crisis and eventually escalating the incident response.

- *How quickly will they it be able to make decisions regarding the report coming from the technical team/CERT?*
- *What countermeasures and recommendations would they take in order to mitigate the escalation of the situation? Are there pre-negotiated policies and SOPs in place?*
- *What would they report to the highest level of the chain of command?*

STRATEGIC/DECISION-MAKER LEVEL – A national crisis should involve all crisis management bodies.

- *Will a state of emergency/crisis be declared?*
- *Are the necessary communication matrices/PoCs in place?*
- *How does the government address the issue of reassuring the public? Does the government have a strategic communication plan in place for such events?*
- *Given a possible international dimension, what will be the official external narrative?*

Academics and students represent a special target group as well. They may be involved both in the form of active players and as part of the exercise planning team. Both options might bring mutual benefit. Internships or direct participation in exercises helps build awareness within the student body. A cyber-aware student body becomes an important resource for future recruitment policies of cyber security institutions.

Understanding the complexity of a cyber incident, and understanding how many various elements and levels are necessary to take into account to tackle it, is the first step to ensuring cyber security preparedness in any given state. A whole-of-nation approach is necessary both in handling real situations and when developing exercises.

Relatively lower exercise participant numbers (20-30) will make for a better “workshop-environment”. In other words, this can provide for a more candid atmosphere stimulating further discussions. Moreover, it will be easier to divide a smaller group into the teams of 4 or 5. Further, the fewer the group total, the easier it is to handle and evaluate performance.

Conversely, you can train larger audiences (80-90) at one time. Such large exercises can also be manageable, but you need to be aware of possible difficulties. If involving dozens of participants, more effort and resources must be allocated to the exercise (money, human resources, facilities, technical requirements, time for preparation etc.). For less-experienced audiences, it is recommended to start with fewer numbers of attendees. Keep the scope of the exercise reasonable.

CONSIDERATIONS FOR SENIOR-LEVEL PARTICIPANTS

Having defined the audience, consider how to address specific participants. Especially when it comes to the highest levels of management, political leaders, and executives, it might be challenging to bring them all to the table simultaneously. Coordination and invitations must be executed well in advance, and should explain the importance and benefits of the exercise. Logistics and organizational issues can be tailored as well. Reduce the length of the exercise documents to their minimum (one-two page summary) and invite the senior-level participants for only the one/two hours when the scenario escalates to their respective level of decision making. Once you have the top-level decision makers on board, let their subordinates brief them and arrange everything needed (just like in real life).

CHAPTER SUMMARY

- In compliance with exercise design and purpose, define the training objectives.
- Determine the training audience and assign tasks following the sub-goals set out in the previous step.
- If you are developing your first exercise, try to concentrate on specific levels/goals rather than devoting all your efforts to the preparation of an all-inclusive exercise.
- The goal is not to include as many participants as possible, but rather to keep the exercise logic, scenario and information flow intact.
- The possible array of participants is wide. Your task is to select the correct blend of participants that relates directly to the exercise purpose/scenario and to make the game beneficial for all invitees.
- Besides how many and what participants, ask yourselves how can you get/convince them to participate.
- Keep the exercise manageable.

CHAPTER 3 EXERCISE NARRATIVE AND INJECTS

EXERCISE NARRATIVE

An exercise narrative drives the story. It should provide participants with a description of an imaginary situation in a geographic environment and at a given time. The scenario usually escalates from simple incidents to more sophisticated ones. The point is to let some serious further consequences and implications occur.

The role of the background story is to create a linking element that encompasses the entire exercise. It also delivers the scenario context to get the game started smoothly. The background story may be divided into several clusters:

- the geopolitical context including geographic location/map, political and historical considerations,
- a list/description of the main actors,
- an initial kick off scenario including a description of past events and current starting position,
- scenario timeline running through the exercise and showing the temporal chronology of events/attacks,
- technical background information,
- media / press-release / news / background information etc.

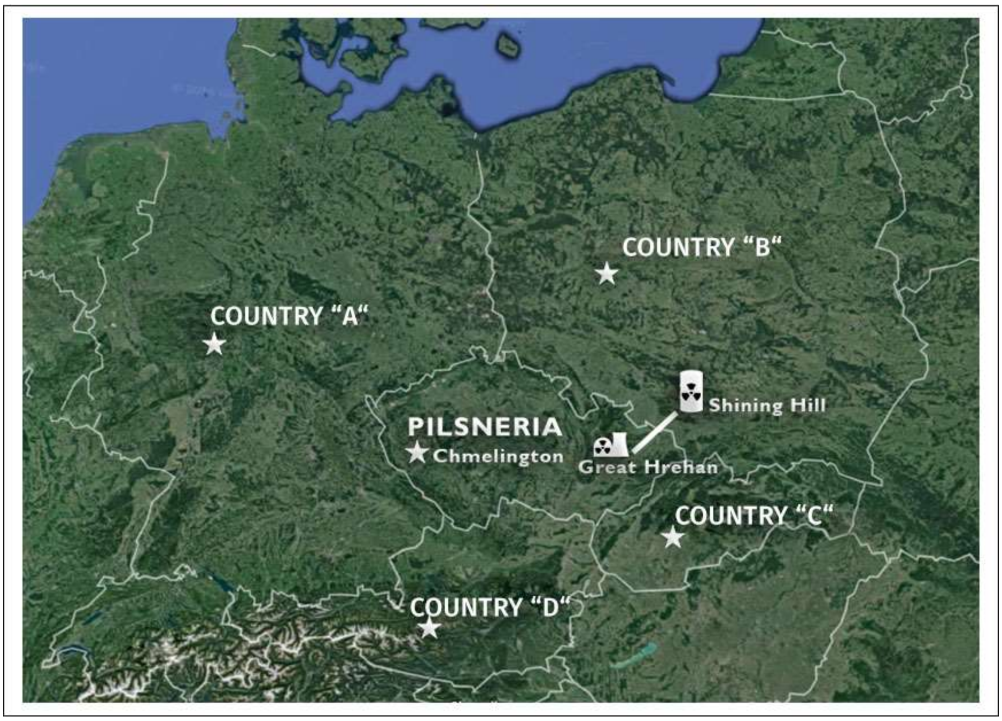


Figure 4: Example of a map used in the Cyber Czech 2017 exercise.

When it comes to the geopolitical environment, the level of realism may vary from complete fiction to reality. The scenario of a table-top exercise based on a hypothetical situation can be fully fictitious. Nevertheless, the more fictitious the storyline is, the more background information should be given to the training audience (including history, politics, demographics, foreign relations, armed forces etc.). Otherwise, a fictional scenario might be difficult to grasp in the limited timeframe and may become more confusing than helpful.

On the other hand, if real geopolitical environment is used, it is expected that basic facts are known (or "google"-able). Thus, exercising a reality-based scenario allows participants to become familiarized with their role more easily. However, there is the risk that if you lose control over sensitive exercise materials and these are released to third parties, this may escalate into real-time diplomatic tensions. For this reason, it is important to mark all sensitive/classified exercise materials accordingly and determine exercise material handling procedures (as defined below). You can also provide a disclaimer explaining the zero attribution and fictitious basis of a scenario (see Appendix).

INJECTS

Just like the initial scenario helps get the exercise started, injects get the game moving forward. Injects or drivers should always have a purpose. They develop the baseline narrative given to the players at the start. You can imagine injects as short pre-scripted messages that provide context and information which will stimulate trainees to do something. They may be used to plot out the story, to speed up, or slow down the play. They may act as additional information, or can include one or more questions to be answered. Additional injects can be made operatively to steer participants in a certain direction.

To maintain storyline consistency, all injects must relate back to the exercise objectives and the road to crisis. Further, injects must not conflict with each other. Well-crafted injects should engage trainees in active discussions or other activity. Clear, grounded, realistic, creative and gripping injects are essential. Responders often tend to claim *"that would never happen that way"*. Creating injects which mirror the real world as much as possible can reduce those complaints. However, if participants continue to fight the scenario and not the problems within the scenario, make it clear that "*you are here to fight the problem, not the scenario".* If necessary, repeat/summarize the current situation, which the participants must address.

Injects should always be customized to the institution/country framework and the environment with which the participants are familiar. Injects should match participant skills and capacity; otherwise, it might be difficult for players to identify with their role and situation. Moreover, exceeding participant capacity can make them feel uncomfortable and demotivated. Be aware that the more the exercise injects reflect a real cyber security framework, the more trainees can get involved in their roles and provide game success.

Once you have a list of vetted injects, you can consider how these will be delivered to your target group, for example by using:

- slides with notes and pictures,
- emails,
- phone calls,
- text messages,
- technical/contextual/threat/situation reports (describing and reporting an incident, providing overall contextual analysis),
- tailor-made audio/video clips,
- real videos,
- authentic photos (even if taken by you),
- radio, TV, or newspapers articles,
- electronic news media outlets,
- social media posts,
- blogposts,
- audio records,
- personal visits,
- message from role-played actors,
- etc.

A combination of the above in realistically designed delivery methods creates a more challenging and engaging experience for training audiences.

Defining a time limit to complete injects and respective tasks is also worth considering in advance. Since dealing with time pressure is a vital and inseparable part of an exercise, choose such deadlines that provide responders time to read assignments and discuss them in the team, but still feel under increased time-pressure. For example, at the beginning of an inject, you may provide participants with more initial time, and then shorten it according to the situation.

Consider the size of the group – the bigger it is, the more time they need to exchange and discuss opinions and views. On the other hand, close-ended questions (e.g. Do you inform media? Yes/No) require less time than open-ended ones (e.g. Would you consider an internationally/diplomatically coordinated response? Elaborate.)

CHAPTER SUMMARY

- **The aim of an exercise scenario is to deliver the right experience, which will engage each participant.**
- **The narrative and injects should be consistent with the overall exercise purpose and objectives.**
- **When developing a scenario, pick a well-balanced level of fiction leading to specific tasks and with sensitivity toward everyone involved in the exercise.**
- **Scripting creative and realistic injects is a must.**
- **Combine methods for how injects are to be delivered to the training audience.**
- **Adjust exercise pressure by both modifying time limits and setting absolute time limits.**
- **Always try to keep consistent and develop an exercise document handling procedure.**

CHAPTER 4
BACKGROUND EXERCISE DOCUMENTS

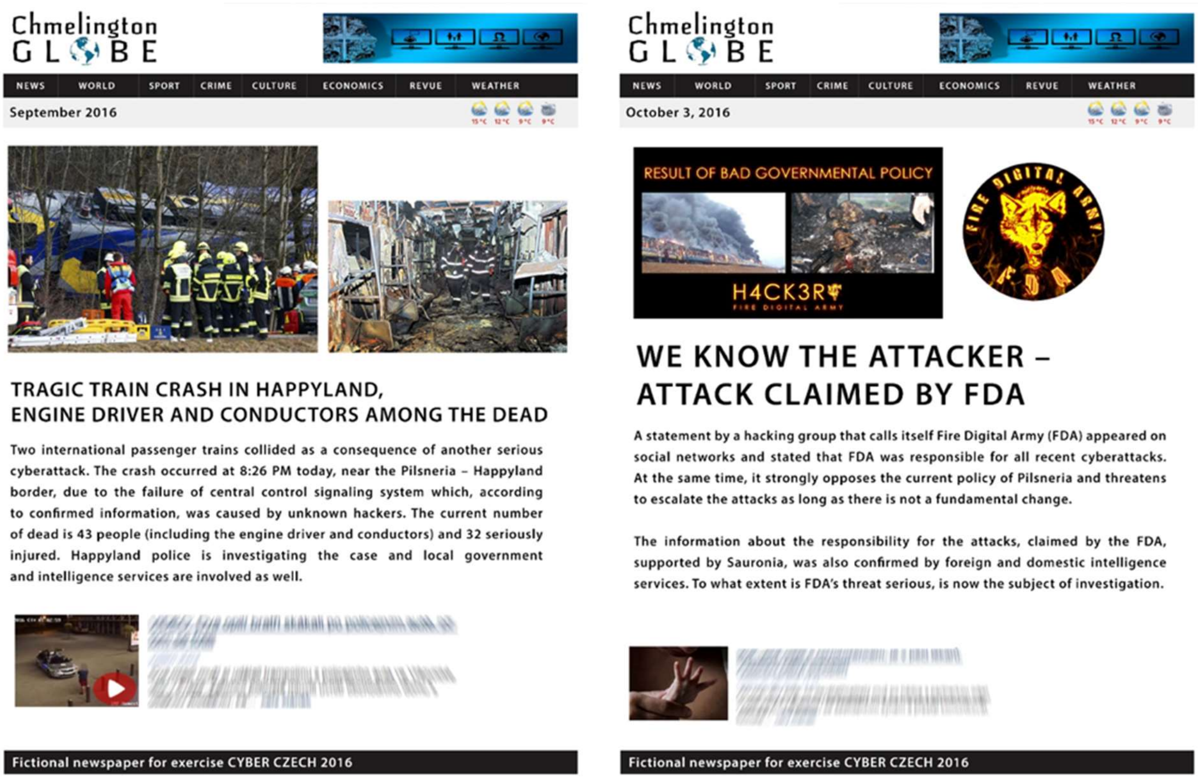
An integral part of each exercise is the creation and maintenance of plentiful supporting documents. The documents are intended to pull participants into the game as much as possible, to ensure realism, and to help players understand the exercise concept and its purpose. Having interesting and clear supporting documents increases the chances of keeping trainees highly tuned to the exercise. These documents can be designed to be fun and engaging, but their primary message should remain to push target groups toward developing solutions to given tasks.

In general, there are several handouts that may be considered; some are required, some are optional. How much of which are required always depends on the exercise concept, type and the complexity.

Supporting documents to be considered for exercise attendees and designers, in order to keep a desirable exercise flow:

- situation manual providing basic information, exercise purpose and objectives, initial narrative, geopolitical synopsis, list of actors (handed out day/several hours in advance to give participants enough time for familiarization);
- instructions and exercise walk-through;
- exercise timeline;
- methods and principles of scoring (if the exercise is scored);
- frequently asked questions (available for the exercise supporting team not involved in the planning stage);
- other practical information[2];
- technical documentation (incident reports, technical environment description, user instruction manual in case of hacked devices, topology – more typical for technical exercises);
- supporting slides telling the story via injects (however, this is not supposed to be a lecture, keep the flow clear and try not to distract the audience by using too many notes/slides);
- answer sheets (for evaluation purposes, keep a coherent numbering system of questions and answers);
- exercise news portal (electronic)/printed newspapers;
- numbers/names of the teams (ready to be put on the table);
- list of the training audience/teams;
- opening videos (to grab training audience's attention, to emphasize, and repeat the main rules);
- exercise agenda (are there any designated coffee breaks or not? What time/day is the hot-wash? – a clear and strict timetable will help visitors better plan their business trip);
- final evaluation questionnaire for participants (given after exercise completion to get as much feedback as possible);
- evaluation presentation (or template ready to be used for a final evaluation briefing);
- other documents, as desired.

[2] Situation manual and practical information create a useful package, which serves as one of the hands-on materials. Thus, it should be available for all participants during the entire game.



Chmelington GLOBE

NEWS WORLD SPORT CRIME CULTURE ECONOMICS REVUE WEATHER

September 2016

TRAGIC TRAIN CRASH IN HAPPYLAND,
ENGINE DRIVER AND CONDUCTORS AMONG THE DEAD

Two international passenger trains collided as a consequence of another serious cyberattack. The crash occurred at 8:26 PM today, near the Pilsneria – Happyland border, due to the failure of central control signaling system which, according to confirmed information, was caused by unknown hackers. The current number of dead is 43 people (including the engine driver and conductors) and 32 seriously injured. Happyland police is investigating the case and local government and intelligence services are involved as well.

Fictional newspaper for exercise CYBER CZECH 2016

Chmelington GLOBE

NEWS WORLD SPORT CRIME CULTURE ECONOMICS REVUE WEATHER

October 3, 2016

WE KNOW THE ATTACKER –
ATTACK CLAIMED BY FDA

A statement by a hacking group that calls itself Fire Digital Army (FDA) appeared on social networks and stated that FDA was responsible for all recent cyberattacks. At the same time, it strongly opposes the current policy of Pilsneria and threatens to escalate the attacks as long as there is not a fundamental change.

The information about the responsibility for the attacks, claimed by the FDA, supported by Sauronia, was also confirmed by foreign and domestic intelligence services. To what extent is FDA's threat serious, is now the subject of investigation.

Fictional newspaper for exercise CYBER CZECH 2016

Figure 5: An example of a fictitious newspaper Chmelington GLOBE in the Cyber Czech 2016 exercise.

Consider in advance which of the documents you want to use. Some can be electronic; some are better reserved for use as printed copies. Moreover, copies may serve as a back-up in case of technology/device failure.

Many prefer printed copies of documents for reviewing the scenario, underlining important text, writing additional notes etc. That said, if participants feel a lack of some critical piece of information, this can be adeptly handled; feel free to explain to the complainant that if he or she were in the middle of a real crisis, he or she would not have all the relevant information/documentation at hand then, either.

Graphic presentation of the exercise and its documents is no less important. Make use of open source graphic tools to make the exercise visually appealing.

CHAPTER SUMMARY

- **Do not underestimate the preparation of supporting documents.**
- **Well-crafted materials are helpful both to exercise trainees and designers.**
- **Think in advance what needs to be printed out.**
- **If a technical solution/tool is used, have a back-up plan in case of failure/power outage.**

CHAPTER 5
MAKE YOUR EXERCISE CATCHY

Exercise execution costs a lot of time, financial, and human resources. To maximize exercise design efforts, some fundamental rules must be followed. If your exercise team's ambitions are higher still, strive to reflect a few more recommended tips. However, keep in mind that each exercise is unique. How polished and well-rounded the exercise ultimately is always depends on the approach of all the people involved.

WHAT IS NECESSARY

- *Well balanced skills testing* – Both technical skills and the strategic, communication and procedural aspects of cyber security must be continually trained.
- *Reflecting a whole-of-nation response* – Cooperation and interaction among public, government and private sector entities is fundamental for managing malicious cyber activities. All communication channels, cooperation agreements and prearranged conditions must be in place before the attacks hit.
- *Involvement of decision-makers and executives* – Strive to incorporate all levels of the "food chain" from the tactical to the operational, and strategic level. Doing so will result in more effective decision making during a complex crisis.
- *Implementing latest trends* – Since cyber exercises are used as an education tool, it is insufficient to exercise only past incidents that your institution has experienced. The latest trends and threats (the unrecognizable or unfamiliar - concepts out of the traditional comfort-zone) must be integrated as well.
- *Emphasis on the evaluation process* – Holding a follow-up session where major stakeholders and players can meet and discuss their results, decisions and feedback is essential. Without participant observations, it is impossible to improve the exercise. Moreover, post-exercise analysis is key for identifying gaps, shortcomings and weak spots, and comparing if any progress has been made.
- *Make the most out of the exercise and its benefits* – Strive to push through the "not interesting" or uncomfortable exercise topics which might tend to otherwise be overlooked. Show, via hypothetical scenarios, what consequences may occur as a result of inadequately addressing an abbreviated or omitted item.
- *Allow friction among different frameworks to discover how they can cooperate during a crisis* – Different stakeholders operate in differing environments (private stakeholders tend to be profit-oriented, versus state sector focus on ensuring the continuity of services), with different tools and mandates/competences. Use the exercise to test if these frameworks are interoperable.
- *Use scenarios which are as realistic as possible* – Responders must feel as though the given incidents are really happening. Ideally, real incidents are selected and then set into a fictitious context familiar to the responders to some extent.
- *Sharing best practices* – Be candid and share outcomes and best practices from the exercises across the security community. The more institutions implement best practices into their real-life operation, the better cyber security is ensured, with a greater degree of commonality.
- *Create a candid and non-threating atmosphere* – Explain to all participants (and top management) that the exercise does not aim to show failures, to seek culprits or to be punitive. On the contrary, it is far more valuable to create a friendly and open atmosphere. Emphasize the opportunity that exercises offer – to

expose trainees to unusual situations and in an interactive way test their reactions and readiness for a real crisis (without the loss of life, money, good reputation or prestige). Moreover, admitting mistakes, and identifying inefficient processes during the exercise is a good practice.

- *Creating adequate pressure* – It is difficult to know the limits of employees when they are exposed to high pressure and stressful situations, prior to their experiencing such conditions. Add more pressure by increasing workload and shortening deadlines for task completion, in order to determine how participants behave in a crisis situation.
- *Distinguish clearly between exercise and real documents* – Avoid inducing panic that might result from forwarding exercise documents to persons not involved in the exercise. It is good practice that all documents and subject lines in emails be marked as "EXERCISE" in a prominent and visible location. Add a note to whom the document may be releasable.

WHAT IS USEFUL AND RECOMMENDED

- *Strategic anticipation* – Exercise designers should be able to come up with a red cell style scenario, which entails constantly implementing new threats and discovered vulnerabilities into the storylines. If your red cell designers struggle with this task, steer them to cooperate with in-house intelligence threat/analytical unit/other experts that handle this kind of information.
- *Open-minded and out of the box thinking* – By integrating (or consulting) technically oriented experts, legal advisors, managers, STRATCOM professionals and analysts during the planning phase, you can enrich the story with nuanced perspectives, dilemmas and difficulties (mostly unknown to the exercise creators).
- *Gripping and engaging scenario* – Generate a scenario based on real attacks, current threats and trends, explore alternative exploits and attack vectors, consider "what if" scenarios. Such hypothetical situations/inputs might galvanize the creation of new disaster recovery plans, standard operating procedures, and/or emergency action plans to mitigate potential cyber security crises.
- *Cyber security as a team effort* – Exercises pose a perfect opportunity to strengthen team work, and build trust and relationships with important counterparts. Make sure you tap into this opportunity.
- *Active involvement of professional journalists* – Do not simulate press and public media actions if the opportunity exists to invite professionals. In return for providing exercise access to the media, they will potentially bring a much-needed element of pressure, stress, panic and urgency. Additionally, following consent and authorization by the exercise design team, journalists can effectively publicize the exercise in their media and thus further spread awareness of its importance among the general public.
- *Consult experts* – It is not the responsibility of exercise designers to be familiar with all areas and determine all challenges that individual institutions face. The responsibility of the exercise designers is to compile the story and develop highly specific injects based on the exercise objectives set at the beginning. E.g. if there is an intent to test the private sector, customize the exercise to the sector´s current needs and framework. To avoid answers like *"this is not how commercial organizations work"*, consult specific aspects of the scenario with your partners from the private sphere in advance.
- *Do not underestimate the value of a test run/exercise review* – Before each exercise, ask colleagues/partners for an

exercise revision. Exercise designers are often too familiar with the plot and know what to expect, and might therefore easily overlook gaps in the process or in the scenario consistency. If conducting technical training or exercises using more sophisticated tools/technology, do test runs first, so as to check that all tools are working properly, the environment is set correctly etc.

- *Visual aspect of the whole exercise* – Graphically unified documents with a proprietary exercise logo, document header or footer will look more professional and advanced.

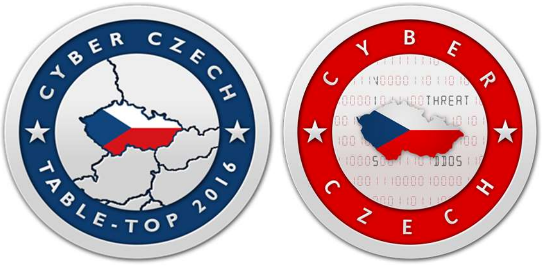


Figure 6: Examples of logos designed for the table-top and technical Cyber Czech exercises.

CHAPTER SUMMARY

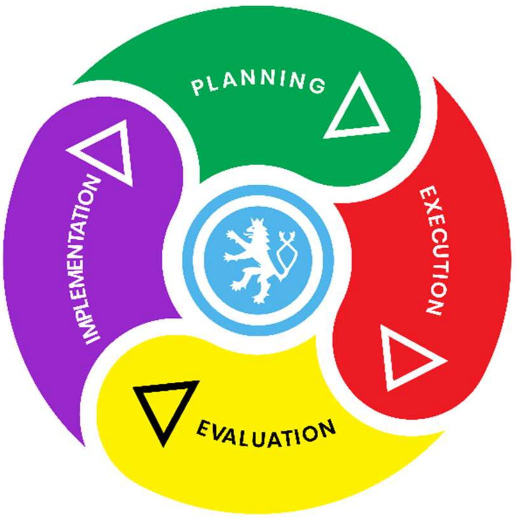
- **Although the exercise offers plenty of opportunities for being innovative and creative, some rules should be observed.**
- **Your exercise can and should be eye-opening and impressive. Draw inspiration from cyber professionals. Exercise results may lead to new technical or procedural innovations.**
- **Invite actual professional journalists and let them actively participate.**
- **Exercise designers cannot cover all of the current knowledge. Allow for consultation with subject-matter experts.**

CHAPTER 6
EXERCISE PLANNING CYCLE AND DESIGNERS

The exercise planning cycle is a continuous process, and therefore a special exercise unit (or at least a designated team of designers who are primarily responsible for planning, running, evaluating, following-up and implementing the exercise results) is required. The most effective and useful cyber table-top exercises are characterized by tailored content and highly specific injects. Preparing such exercises requires a lot of human resources, time, knowledge and experience in project management and coordination skills. A major task-set for creators is to determine the exercise purpose, and to develop the pertinent story with subsequent injects. To be able to do this effectively, exercise designers need to gather inputs from relevant colleagues and partners. To validate that the narrative and injects are oriented in the right direction, consultations with the correct professionals is necessary. For instance (depending on the training objectives) ask a legal advisor on legal implications, ask the STRATCOM team to get insight into strategic communication areas, ask experts on crisis management regarding overall procedures and crisis processes, ask technicians about technical aspects, ask foreign affairs/specific region analysts on geopolitical considerations, etc.

The preparation of cyber security exercises is about people. Organizational skills and attention to details are a must for exercise designers. They must be creative, innovative, and open to new ideas. The more novel the exercise is, the more participants can take away from the training. Precision and strict adherence to schedule is another required skill, as is the preparedness to be ready to absorb lots of information. Exercise unit members should have the opportunity to meet regularly, to hold briefings and conferences with applicable colleagues and parties during the entire planning stage. Good communication and argumentation skills are also very valuable.

To illustrate all that the preparation and execution of an exercise entails, please refer to the following table and graphic (Figure 7). The table, apart from underscoring the continuous planning process, divides the main activities into administrative, organizational and content portions.



ADMINISTRATION

- Initial needs analysis
- EXE's planning
- Budget
- Human resources
- Competencies
- Technology
- Equipment
- Paperwork
- Cooperation
- Agreements with involved parties

ORGANIZATION

- Type
- Main purpose
- Training objectives
- Training audience
- Timetable
- Division of roles
- Limitations
- Consultations
- Coordination
- Visitors and media coverage
- Participants feedback
- Following-up
- Implementation

CONTENT

- Background story
- Injects
- Briefings
- Supporting documents
- Visual materials
- Motivation
- Feedback questionnaires
- Scoring
- Evaluation methodology
- Observations and takeaways
- After action report

Figure 7: Planning cycle.

From the outset, determine boundaries and limitations (budget, human resources, time, travel, technology costs, and other resources). Pre-exercise analysis is another important step. What is the overall purpose? What is the intended training audience? What should be exercised, and how? When and where should the exercise take place? The third column of Figure 7 sums up what else must be developed in order to create an interesting and catchy exercise. Start with training objectives, elaborate on scenario, mix it with past incidents, current trends, and strive to include anticipated developments and a few "hot topics" to engage players as much as possible. E.g. while the issue of drones is becoming mainstream, artificial intelligence, robotics and autonomous devices are creating the headlines these days. Split the scenario into smaller logical clusters, main events and specific injects and tasks. Take care to consider the aspect of motivation. Encourage motivation by tailoring an exercise to the training audience needs, capacities, and framework and by setting the storyline into a realistic environment. Be ready to provide hints in case the audience becomes side-tracked. Create a friendly atmosphere and keep repeating that an exercise is not an exam, but an opportunity to expose players to an unusual but possible crisis scenario.

A dedicated exercise management portal or tool can be highly useful for the better coordination of tasks. However, for the needs of a limited-time table-top exercise, a common checklist may suffice just as well. Assign roles and tasks, and determine deadlines. Try to keep to a reasonable time frame.

A crucial part of every exercise is receiving feedback from participants, evaluating responses, reporting to leadership and implementing (wherever feasible) all findings and lessons learned into the real world.

CHAPTER SUMMARY

- **Planning and execution should always be followed by the evaluation and implementation stage.**
- **Since this is a long term-process, a special unit/group of employees should be dedicated to organizing cyber exercises.**
- **Provide education to exercise designers not only in the cyber field, but also in project management.**
- **Engage decision-makers with insufficient cyber knowledge (but not only them) by involving hot topics they know from the media.**
- **Make a checklist.**
- **Check and double-check everything.**

CHAPTER 7
EXERCISE EVALUATION AND FOLLOW-UP

The evaluation stage is an integral part of the exercise planning cycle and should reflect on the exercise purpose and objectives. Thus, the evaluation work begins already during the planning phase. The exercise team should key in on several questions: *What do you want to achieve with the exercise? How will evaluation be done? According to which matrix, methodology, and criteria will the exercise be assessed?* If you do not know what you want to measure, assess or compare, it will be difficult to ask the right questions.

There are two basic purposes/levels of an evaluation:

The first one tells us how to improve the planning process and the exercise itself. It is based on the exercise creators' observations and participants' comments about the organization aspects of the exercise. This kind of feedback helps organizers better customize exercises to specific audiences and make exercise documents more comprehendible for them. Based on participant responses, the exercise can be designed so as to cover the issues and topics most relevant to them. Questions asked should focus on areas of improvement and aspects of overall exercise design.
This is the right place to ask players about whether they thought the scenario and injects were challenging and realistic, what worked and what did not.

Sample evaluation questions:

- *Was the exercise design realistic?*
- *Did the scenario accurately reflect real-world examples?*
- *Were the exercise documents and visual materials complete/useful?*
- *Were the main events and injects structured and well-organized?*
- *Was the introductory presentation helpful in understanding exercise objectives?*
- *Did trainees feel under pressure and stress?*

The second level of evaluation emphasizes systematic assessment of the exercise objective(s), examination of injects and results, and overall responder performance. Put simply, this type of evaluation focuses on bullet points covered in the "content" part in Figure 7 (previously introduced). The goal is to determine how participants managed to treat the individual tasks and to what level they performed (low-standard, average or superior). More importantly, it brings to light the strengths and weaknesses, gaps, and shortcomings captured when dealing with a complex crisis scenario.

Sample evaluation questions:

- *List improvements that need to be made to plans and procedures for responding to the exercise crisis scenario.*
- *List plans, processes or procedures that should be developed, reviewed or revised based on the exercise findings. For each point, indicate who or what agency/unit should be assigned responsibility for implementation.*
- *What lessons learned have you identified from the exercise regarding the content aspect?*
- *Is there anything in particular you would like to see in future exercises?*

In order to compile all participant notes and observations, the target audience can be required to fill out specific questionnaires after the end of the exercise *(see sample evaluation questions above)*. In addition, interviews with key players and observers may be helpful. Again, all questions articulated here must be in line with exercise objectives, evaluation metrics and criteria to reveal the greatest challenges and pitfalls. Inputs for evaluation should be gathered during the hot-wash. This is largely a guided discussion, involving organizers, designers, evaluators, observers and participants, aimed at providing an opportunity for all to express overall impressions, concerns and views.

Some of the basic principles for achieving an objective assessment of the current state/performance include a frank and open assessment of actual conditions. This is especially relevant in cases of poor performance or failure, when leadership might not be willing to accept anything less than good news. Evaluation should always be considered a way of pinpointing areas for/of improvement, rather than an excuse for blaming or finger-pointing. The goal is to further sharpen participant skills, broaden their experiences and fill gaps identified during the exercise. So as not to give the impression of blaming, evaluations should always contain potential solutions to the identified shortcomings.

Evaluation outcomes emerging from feedback and debrief sessions should be further elaborated in an After Action Report (AAR). Take your time with preparing this summary report (it usually takes several weeks). A high-quality AAR describes the exercise, what the main objectives were and if (and how) they were met. Key aspect of the AAR include highlighting the major weak spots and giving recommendations on how to minimize or eliminate shortcomings observed in the exercise. Without drafting solutions and countermeasures, the AAR (and even the whole exercise) loses its potential to serve as a key supporting tool in promoting the remedy of insufficiencies and driving organizational change (at management and/or political levels).

Another means for following up on emergent issues is to organize a follow-up event, invite respective decision-makers, top management and political leaders, detail key weak spots and jointly discuss possible solutions. It is always better then if the executives have gone through the scenario and experienced the virtual negative consequences of a scenario which ended up poorly. However, it is also critical that the right people be present - people with the power to move things forward. Provide these people with the AAR to have something to refer to.

The evaluation process and follow-up event should lead to the creation of a best practices document which constitutes an important part of each exercise. Its purpose is to outline what to do in case of such a crisis/scenario, to serve as a step-by-step manual in dealing with serious incidents. As the best practices document is one of the most useful and practical outcomes for the participants, make it available to your partners and other stakeholders. The more people and institutions are familiar with this document, the more educated and prepared the community it is.

Finally, the essential implementation stage remains to be addressed. Once you have identified weak spots and have produced an AAR and best practice summary, it is time to implement all of the findings into real life wherever feasible. It is likely that cyber exercises will uncover insufficiencies in current procedures, process, SOPs and policies triggered in the wake of a cyber incident. Lay out the standard operating procedures, business continuity plans, disaster recovery plans on the table, assess their adequacy and revise them to avoid the same shortcomings. Develop a plan B for all possible scenarios. Do not neglect to educate senior leadership and other applicable audiences regarding the possible risks and threats.

What to exercise next time? Test and validate whether all revised plans and procedures would suffice and work in a cyber crisis. Find out what progress has been done in this area.

CHAPTER SUMMARY

- **Planning and evaluation stages should be devoted the same effort.**
- **Use the exercise output not only to improve the exercise itself, but also to make real processes more effective.**
- **Report to leadership about the exercise findings in a suitable way.**

CHAPTER 8
SUMMING IT UP

Well-crafted and well-executed exercises are proven to be valuable and effective tools for raising cyber security awareness among senior leaderships, managers, and IT professionals. Exercises with integrated operational and decision-making components can serve to test real-world procedures, communication flows and improve decision-making at strategic levels, as well as to enhance the technical skills of cyber security operators.

Exercises are perfectly targeted at the human element which poses the weakest link in the security chain. However, the aim of exercises is not to expose individuals to stressful situations and to punish them if they fail. Nor is the aim to publicly expose institutional gaps and jeopardize institutional reputations. On the contrary, the benefit of exercises lies in the opportunity to educate personnel and improve the functioning of institutions in an exciting way. Additionally, an exercise fiasco does not necessarily mean a disaster. It can identify an issue to be addressed before an actual emergency occurs. Hence, from this perspective, sometimes failure might be better than success. Demonstrative and engaging exercises enable participants to take away more knowledge and experience than from the most dense and comprehensive lecture.

It is the intent of this handbook to provide useful guidance and practical advice for designing and carrying out such cyber table-top exercises.

GLOSSARY

AFTER ACTION REVIEW

AAR provides a structured brief overview of the exercise, major strengths demonstrated during the exercise, and areas that require improvement.

CYBER RANGE

A virtual environment that is used for cyber security exercises with a technical element, cyber technology research, and development. It provides a unique platform and tools for testing and analyzing security threats to critical information infrastructure and other important systems. It is capable of creating various scenarios involving extensive computer networks running services and applications, and thus facilitates the detailed study of the emergence, spread, and impacts of current cyber threats.

HOT WASH

A debrief conducted immediately after an exercise or test with staff and participants.

INJECT

Pre-scripted events that simulate and include directives, instructions, and decisions. Exercise controllers provide injects to exercise players to drive exercise play towards the achievement of objectives. Injects can be written, oral, televised, and/or transmitted via any other means.

TABLE-TOP

A meeting to discuss a simulated/hypothetical emergency situation. Table-tops are used for testing emergency plans, clarifying roles and responsibilities, decision-making processes etc. They should result in action plans for continued improvement of internal processes and emergency plans.

THREAT ASSASEMENT

The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or human-made, which have or indicate the potential to harm life, information, operations, and/or property.

TRAINING AUDIENCE

An individual, group of individuals or organization that performs a particular task or set of tasks during the execution of the exercise.

APPENDIX

EXAMPLE 1: MAIN EVENT AND INJECT

MAIN EVENT X

INJECT X.1 A week before the general elections in Country A, the Centre Party becomes victim of a cyber-attack. They have lost control over their mail services and website. It is now showing defacements, damaging the image of the party. The Centre Party is considered to be the most pro-country B of the major parties, supported by many people from Country A as well.

QUESTIONS:

X.1.1 Would you recommend providing help to the Centre Party? Who could make such a decision?

X.1.2 How would you justify such a decision in the eyes of the other political parties and public?

X.1.3 Should Country A offer help to all political parties in case of need?

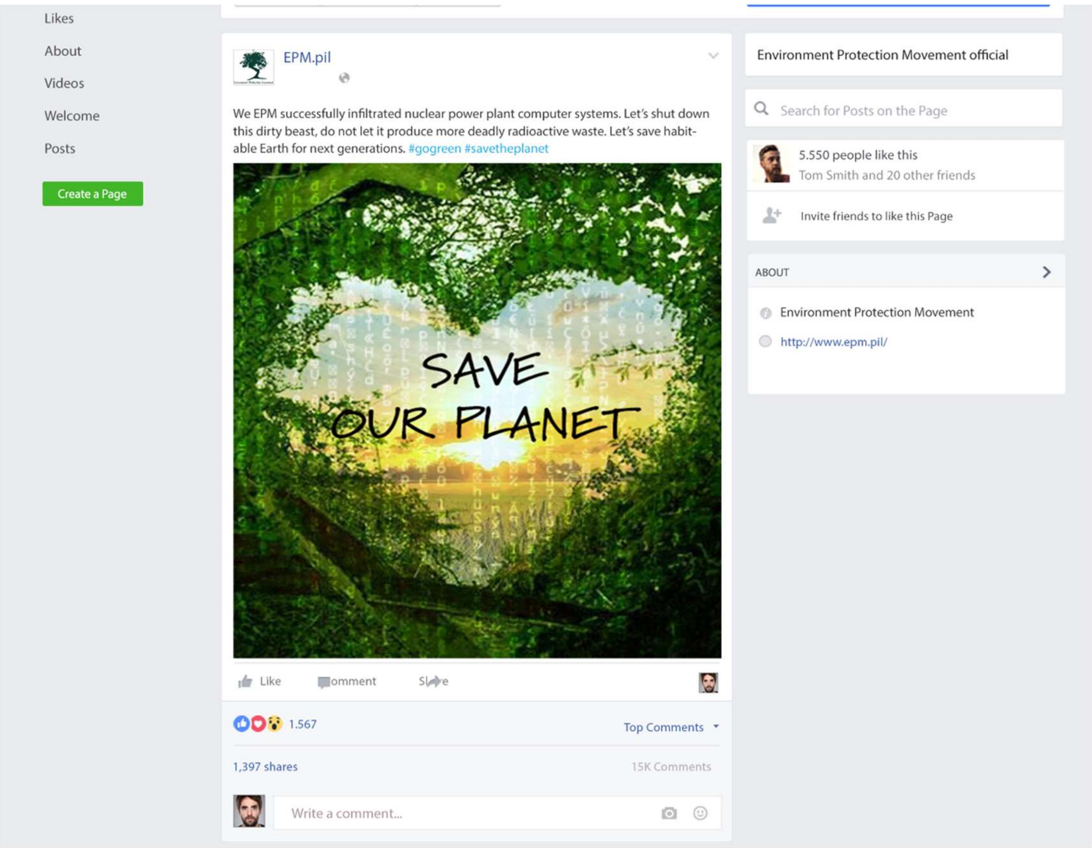
X.1.4 In your opinion, what might be the reputational impacts on the electoral system and government, if unable to ensure a smooth run of pre-election campaigns?

X.1.5 Would you consider postponing the election? If yes, elaborate on that.

Answers:

EXAMPLE 2: AN INJECT DELIVERED IN THE FORM OF SOCIAL MEDIA POST

(Context is fictitious).



EPM.pil

We EPM successfully infiltrated nuclear power plant computer systems. Let's shut down this dirty beast, do not let it produce more deadly radioactive waste. Let's save habitable Earth for next generations. #gogreen #savetheplanet

1.567

1,397 shares

15K Comments

Environment Protection Movement official

5.550 people like this
Tom Smith and 20 other friends

Environment Protection Movement

http://www.epm.pil/

EXAMPLE 3: DISCLAIMER STATING THE LEVEL OF FICTION AND ATTRIBUTION

“Although some events depicted in this exercise are based on real incidents/occurrences, the exercise is fictional and does not intend to link any nation/state/government/group of individuals to any actual wrong doing. Nor does this exercise serve as an attribution tool. The use of nation states and other actors, as well as events, locations, incidents and attribution hints are purely fictional.”

ABOUT THE AUTHOR

Martina Ulmanová is the Head of the Exercise Unit at the National Cyber and Information Security Agency of the Czech Republic. She has extensive experience in the field of cyber security exercises. In her role, she is responsible for cyber security exercises at the national and international level run by the Czech Republic. Since 2014, she has served as an exercise director and local trainer for the Czech Republic in CYBER COALITION, a NATO cyber security exercise. In 2017 she became a leader of one of the exercise planning sub-teams in the world´s largest cyber defense exercise, LOCKED SHIELDS.

She is involved in the preparation of and lecturing for university courses on cyber security. In addition, she coordinates and prepares cyber awareness campaigns including e-learning projects and cyber training for special target groups. She holds a master´s degree in Strategic and Security Studies from Masaryk University in Brno, Czech Republic.

Martina Ulmanová
Head of Exercise Unit
National Cyber and Information Security Agency
Mučednická 1125/31, 616 00 Brno, Czech Republic
e-mail: m.ulmanova@nukib.cz
www.nukib.cz
Twitter: @GovCERT_CZ