Cyber Security Decision-Making Exercise: Solution for Businesses

The Need for an Effective Decision-Making. Today, the possibility of large-scale cyber-attacks against wide range of targets from nation states to companies and individuals is widely recognized. Decision-makers, including business leaders, upon who falls responsibility for action in a cyber-emergency are often deprived of prior experience or preparation, potentially hampering the effectiveness of responses. One of the key problems for governments and private enterprises in countering the cyber threat is the lack of understanding about how interconnected and vulnerable our networks and critical services are.

Another key challenge is the lack of effective decision-making processes. The cyber security exercise developed by BHC Laboratory enables the shaping and testing of strategic- level decision-making processes during a cyber-emergency. Our solution is based on extensive experience in conducting strategic exercises. Our goal is to train also business leaders, because cyber security is not merely a technical problem, the key to effective response often lies at the management level.

Picture 1. EU CYBRID Exercise for EU Ministers of Defence. 7 September 2017, Tallinn, Estonia.

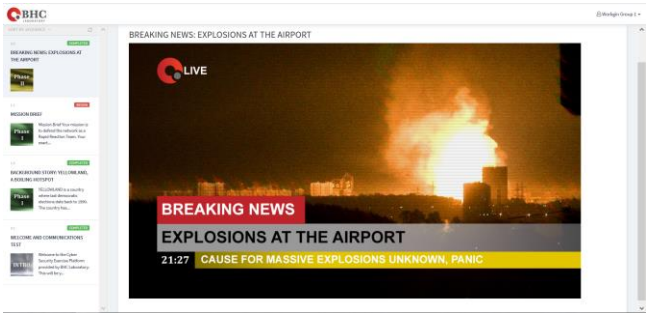
Exercise as a Tool to Test and Improve Regulations. The particular emphasis of this Exercise is on decision-making procedures and related decision-making frameworks. The Exercise shall motivate participants to discuss and understand the divergent and often-conflicting issues associated with decision-making in a cyber- emergency as well as the consequences of the choices made to the enterprise, business process or even to the nation as a whole. It is also an ideal tool to assess and compare the respective procedures and understanding thereof between various stakeholders. Its prime purpose is to elucidate the nature of cyber-threats, by identifying potential challenges and difficulties and, ultimately, by inspiring thought-provoking discussions and advancing the quest for novel solutions.

The Strategic Decision-Making Framework. The cornerstone of the exercise is focusing on key analytical questions in relation to decision-making processes the point of view of the strategic decision-maker, a business leader – as opposed to that of an operative, technical specialist:

TIMELINE – what is a realistic timeline to organize and implement an effective response? How far ahead can risk mitigation and business continuity plans be made in enterprise cyber security?

COOPERATION – who are necessary partners and allies to carry out effective defence of your business? Are current cooperation mechanisms working? What are the necessary new cooperation frameworks to ensure an effective response? What is the role and responsibilities of the private sector in working with government to achieve effective defence?

TRANSPARENCY – what is the required level of secrecy/transparency to carry out an effective cyber-defence? What information is suitable for public dissemination? How to deal with the ever changing rules of protection of data, commercial secrets and even state secrets? How to deal with media requests including leaks and fake news?



Picture 2. Transparency and media relations are one of the aspects tested in the exercise.

AUTHORITY – what crucial decisions need to be made and by whom during a cyber attack? Are existing decision-making processes working and effective? Is there sufficient or too much regulation/planning? And finally, who is responsible for taking the decision in a particular situation?

The Exercise Set-up. The Exercise enables participants to play their assigned roles in the company during a simulated large-scale cyber-attack. The participants can either form one company that is divided into different parts or play several companies at the same time. The exercise can be carried out simultaneously in various countries. This scalability allows for exciting comparisons, correlations and actual results to devise effective management responses to cyber-attacks. Participants are tasked with taking decisions and collaborating with each other. The decision-making process is monitored, assessed and if appropriate, countered by the Exercise Management Team. This is to preserve authenticity, keep the exercise flowing or to challenge participants.

The Outcomes and Benefits. The Exercise is designed to yield the following outcomes and benefits:

- Enhanced knowledge and understanding by participants of the nature of the threats emanating from cyberspace.

- A better understanding by participants of decisions that business leaders need to take during a cyber-emergency. By enacting rigorous real-life scenarios, participants obtain indispensable practical knowledge of the requirements for mounting a successful cyber-defence of an enterprise. This knowledge can also be employed to compare and contrast the various defence systems currently in existence.

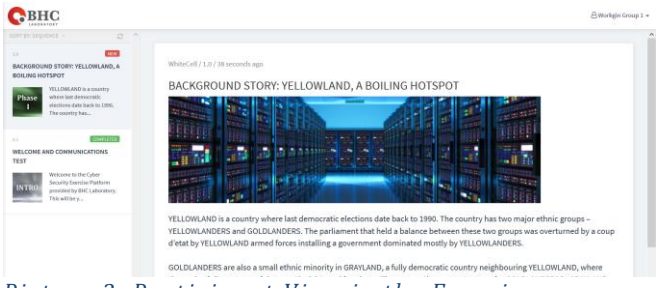
- Fuller understanding of the regulatory framework through identification of shortcomings in risk management, but also legislation and organization in the field of cyber security. In particular, one of the goals of the Exercise is to inspire new proposals for strengthening the regulatory framework.

- Testing the efficacy of draft regulations, contingency and cooperation plans, even budgets and business plans from cyber security perspective – concerning which there are various ongoing initiatives – by comparing these to potential alternatives.

- Enhancement of the horizontal cooperation within organization, between companies and even at national and international level. During the exercise, participants will be instructed to create cooperative networks that may prove useful in future response scenarios.

- Better understanding by business leaders of the actual impact of their responses. One of the strengths of the exercise is its strong methodological base that takes into account the specific audience of decision-makers and specific interests, issues and challenges that such composition of audience brings along. We have addressed the following key challenges, described in detail below to bring about a successful exercise.

Technical Set-up of the Exercise. The exercise is carried out on a proprietary exercise management tool. The tool is highly scalable, very intuitive to use and can simultaneously support very large number of participants across the globe. The tool has effective and instant feedback module that makes it engaging not only to participants but also observers. Its data capture functionalities ensure that exercise discussions will not be lost and can be used for later in-depth analysis. The exercise is usually accompanied by a feedback session where main events, decisions and reactions are analyzed. This ensures



Picture 3. Participant View in the Exercise Management Tool.

participant engagement and truly effective learning experience.

References. This exercise solution is internationally proven and highly recognized. It has been used at very high profile international exercises for international organizations, national governments, training institutions and large corporations. The sample events include: EU CYBRID Ministerial Exercise for European Defence Ministers; NATO Locked Shields Strategic Track (2016, 2017); National Strategic Cyber Defence Exercises carried out at the request of the European Defence Agency in Portugal, Greece, Czech Republic, Austria, Latvia, Slovenia and Cyprus; the National Cyber Security Exercises of Estonia, Portugal, Moldova (funded by United States State Department), Georgia, Colombia, etc.