Secura
A BUREAU VERITAS COMPANY

Tabletop Cyber Crisis Management

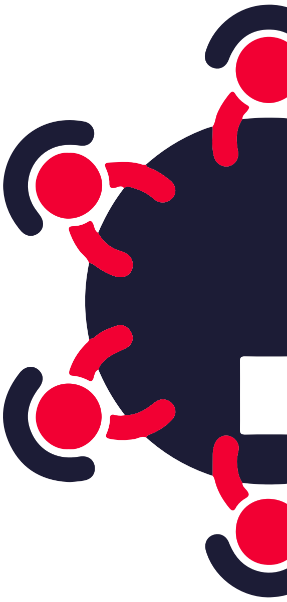
Cyberattacks appear in the news every day. Organizations are increasingly aware that being well prepared is essential. The question is no longer 'if' an organization will be attacked but 'when'. What do you do in case of an attack?

During Secura's Tabletop Cyber Crisis Management workshop, operational procedures for dealing with such an incident will be practiced and evaluated using a realistic scenario. These scenarios and our approach are based on NIST standard SP 800-84 to effectively prepare and execute cyber incident exercises. Employees involved in the first phase of a cyber crisis within the ICT chain in an incident such as ransomware will be trained through the tabletop crisis exercise.

Good Preparation is Half the Battle

Do you know if your organization is well prepared for a cyberattack? Who are the first points of contact? What are everyone's responsibilities, and what can be expected from each other? How quickly can you intervene, and what are the follow-up steps? Secura has designed the Tabletop Cyber Crisis Management to map and assess these processes. During the tailored workshop, a ransomware scenario will be discussed, whereby the following learning objectives for the participants will be addressed:

- Identify and analyze issues during the simulated incident.
- Collaborate within the team to arrive at a balanced approach.
- Execute internal procedures to deal with ICT security incidents and ICT emergencies.
- Scaling up and cooperation of participants and coordinators to reach a solution.
- Insight into different roles during a crisis.



How does it work?

The Tabletop Cyber Crisis Management is an interactive workshop with lots of information, simulated reports, and evaluations to learn how to act effectively together during an incident. The exercise also contributes to team building and developing mutual respect. The training workshop is useful to improve cybersecurity skills and become better aligned as an organization for other incidents.

01

PREPARATION

KICK-OFF MEETING & COLLECTION OF RELEVANT DOCUMENTATION

During the preparation, Secura agrees with you on the final scope of the exercise, our approach, the planning, and the desired results. With your knowledge, we will collect the proper documents about the IT environment and the crisis infrastructure within the organization.

02

CRISIS TRAINING

INTRODUCTION TO RANSOMWARE & CRISIS PROCEDURES

The ransomware tabletop begins with an introduction to the concept of ransomware. How does a ransomware attack work, and which parties are involved? What threat does it present to your organization? The second part of the training focuses on your organization's crisis process. It is the starting point of an interactive discussion about the extent to which these processes are up-to-date for a cyber incident within your organization.

03

CYBER CRISIS EXERCISE

SUPERVISING THE EXERCISE & IDENTIFYING IMPROVEMENTS

The final part of the tabletop is built around a simulated incident where the participants conduct a crisis consultation in two rounds. We confront the participants with a challenging but realistic cyber scenario to test mutual collaboration and coordination. We prepare the crisis exercise and provide simulated notifications during the exercise, supervision, and observation. During the exercise evaluation, we look at the possibilities to improve the crisis approach.

04

EVALUATION

EVALUATION IN COOPERATION WITH THE ORGANIZATION

After the tabletop exercise, Secura provides a memo of the observations made during the training and the exercise. This contains the learning lessons from the exercise and recommendations for the (cyber) crisis team that can be used to improve incident response and crisis management within your organization.

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today!

Follow us on:

☎ +31 88 888 3100
✉ info@secura.com
secura.com

BUREAU VERITAS
1828

Shaping a World of Trust