Secura
A BUREAU VERITAS COMPANY

Tabletop OT, DRP & Cyber Crisis Management

Cyber-attacks appear in the news every day. They can seriously impact the processes of Operational Technology (OT) and Industrial Control systems (ICS). Being well prepared is essential. A Tabletop exercise helps you prepare your response to a cyber-attack. It can also help you perfect your OT Disaster Recovery Plan and Crisis Management Plan.

Are you prepared?

Is your organization prepared for a cyberattack or a large-scale security incident on its OT systems? Does your team know what to do and how to recover when all Operator Interfaces (HMIs) are unavailable? What is the impact on production or safety? What are everyone's responsibilities? Is external support from the ICS vendor required? Who are the first points of contact?

Practicing for disaster

You don't want to look for the answer to these questions during an incident. Secura can help you prepare. During a Tabletop OT DRP & Cyber Crisis Management workshop, you will practice operational procedures for dealing with such an incident. This interactive workshop simulates a realistic high impact cyber incident on the OT systems, for example a ransomware scenario.

This exercise trains employees in all the phases of a cyber crisis, from the first initial detection to final remediation. Think of this as the cyber equivalent to the annual fire drill.

The goal of the Tabletop is to help participants to:

- Identify and analyze issues during the simulated incident.
- Collaborate within teams to arrive at a balanced approach.
- Execute internal procedures to deal with OT/ICS security incidents and emergencies.
- Scale up and cooperate to reach a solution.
- Gain insight into different roles during a crisis.

The exercise also checks current plans and procedures. This means you can:

- Verify if the plans cover large-scale OT incidents.
- Identify gaps in strategies for backup, restoring, security monitoring and disaster recovery.
- Improve your strategies, using our observations and recommendations.

The scenarios and our approach are based on NIST standard SP 800-84 to effectively prepare and execute cyber incident exercises.

How does it work?

Over the course of the exercise, the participants will receive information, simulated reports, challenges, and situation developments that contribute to the scenario. During the simulation we will take the time to evaluate the steps taken during the simulation. The participants learn how to act effectively as a team during an incident. This means the exercise also contributes to team building and developing mutual respect.

PREPARATION

KICK-OFF MEETING & COLLECTING RELEVANT DOCUMENTATION

During preparation, we jointly determine the scope of the exercise, the planning, and the desired results. We will collect the documents and information about the OT environment, such as OT system diagrams, the OT disaster recovery plans and the crisis infrastructure within the organization. The scenario will be tailored to the specific OT network and organizational structure in scope. Based on the defined goals and content of the exercise we can determine the required participants, like OT, IT, Management, or vendors.

CRISIS TRAINING

INTRODUCTION TO HIGH IMPACT OT INCIDENTS & CRISIS PROCEDURES

The tabletop begins with an introduction of high impact OT cyber security incidents. Secura gives a presentation about ransomware and the threat it can pose to your organization. The second part of the training focuses on the crisis process and disaster recovery in your organization. We engage participants in an interactive discussion about the current processes within your organization and whether they are up-to-date.

CYBER CRISIS EXERCISE

SUPERVISING THE EXERCISE & IDENTIFYING IMPROVEMENTS

The main part of the tabletop is built around a simulated incident in which the participants conduct a crisis consultation. The simulated incident covers everything from initial detection of a small security issue to the full-scale escalation, crisis management and disaster recovery. Secura provides supervision and simulated notifications. The exercise is divided in two to four rounds; after each round we evaluate and discuss.

EVALUATION

EVALUATION IN COOPERATION WITH THE ORGANIZATION

After the tabletop exercise, Secura writes a report which covers the observations made during the exercise. This contains the lessons learned from the exercise, potential gaps in the current Disaster Recovery and Crisis Management Plans, and recommendations for the (cyber) crisis team that can be used to improve incident response and crisis management within your organization.

The role of a DRP and CMP in the tabletop

During an OT Tabletop, a cyber incident escalates to a disaster. This means the exercise works best if you already have a Disaster Recovery Plan (DRP) or a Crisis Management Plan (CMP) in place.

OT DISASTER RECOVERY PLAN

A Disaster Recovery Plan, or DRP, is a comprehensive plan that covers full recovery of the OT network, including the industrial controllers, SCADA systems and other vital components. Recovery order, system dependencies, required resources and tools, reliable backups, tested procedures and validation processes are all required for a successful and fast recovery.

During the preparation of the OT Tabletop, we check whether this plan exists and is successfully implemented. If you do not have a DRP, Secura can provide support to review or create one, based on relevant controls specified in NIST CSF and IEC 62443-2-1 and matched to the current infrastructure.

CRISIS MANAGEMENT PLAN

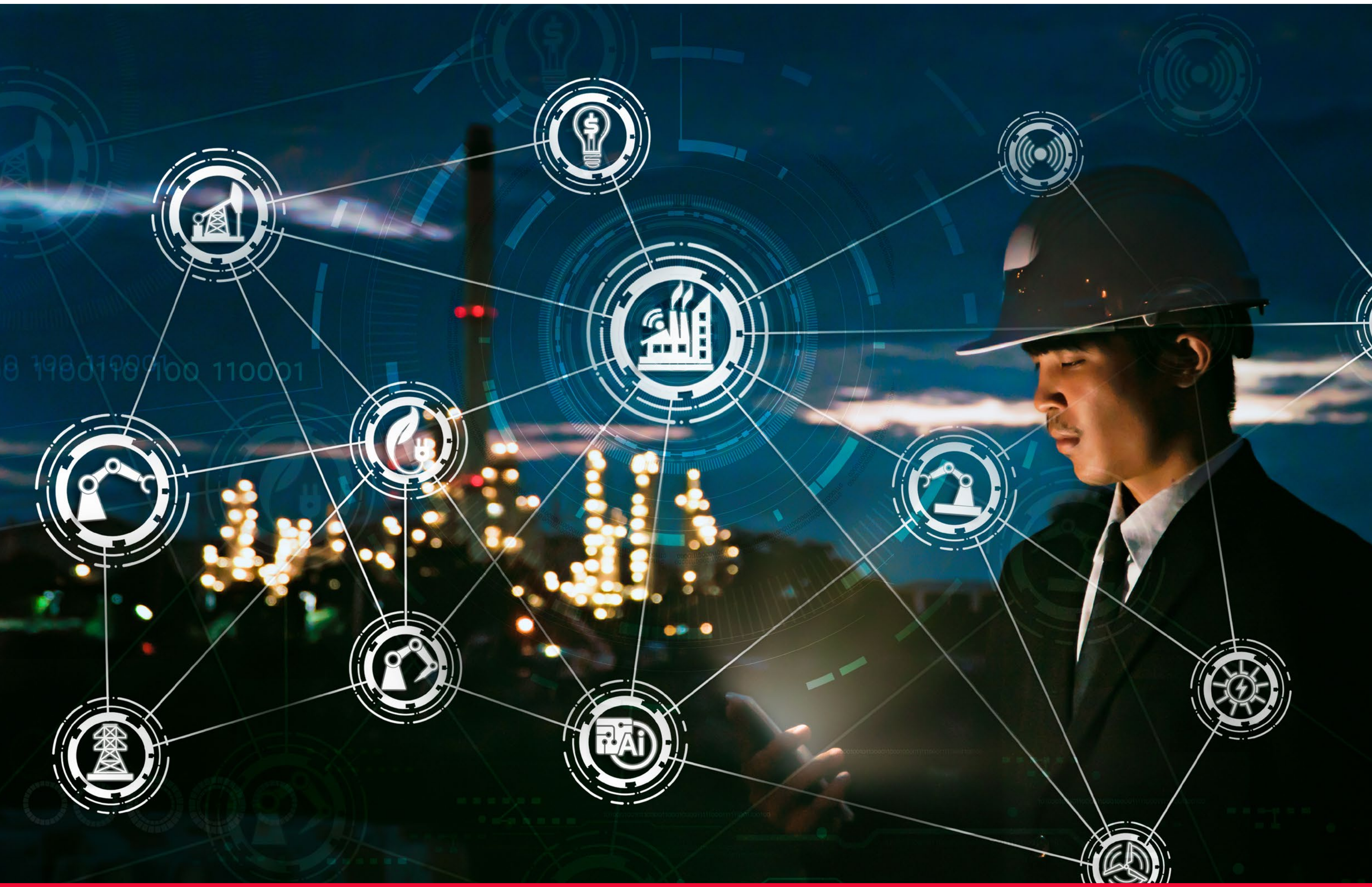
A Crisis Management Plan, or CMP, is all about managing the crisis on a company level, including decision-making and communication. Most organizations have a general plan, but they don’t always cover disasters caused by cyber and/or cyber incidents in OT.

During the Tabletop we will review the existing CRM. If needed, Secura can help you improve or create this plan.

Your challenges in OT

Secura is aware of the challenges within many OT environments. Very often the responsibilities are less well defined than the IT part of an organization. At the same time ICS systems can be complex. They can also directly impact primary business processes, the physical environment or safety.

Another issue is this: most organizations lack dedicated OT security specialists. OT automation engineers or instrumentation engineers don’t always have the necessary expertise to deal with complex security issues. At the same time, the IT security-specialists within an organization might not have the necessary expertise to deal with a complex OT environment. This increases the importance of a solid and verified plan.



Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

☎ +31 88 888 3100

✉ info@secura.com

secura.com

BUREAU VERITAS 1828

Shaping a World of Trust