TABLETOP EXERCISES

TEST AND OPTIMIZE YOUR RESILIENCE

AwareTec GmbH

Content

Executive Summary

Given the ever-evolving landscape of cybersecurity threats, organizations must continuously improve their readiness to respond effectively to potential security breaches and attacks. Tabletop exercises go beyond predetermined discussions and offer a realistic approach that reflects the complexity of real-world incidents.

This booklet presents a modern approach to cyber crisis training: a combination of realistic simulations, scenario-based role-playing, and playful elements to fully engage both technical teams and corporate decision-makers.

Our tabletop exercises are based on current threats and evolving regulations such as NIS2 and DORA, allowing companies to test not only their technical defenses but also the responsiveness of their executives and their compliance readiness.

By integrating tabletop exercises into your cyber strategy, you leverage post-incident analysis, and you get an in-depth look at your strengths and weaknesses—along with practical, prioritized steps for improvement.

CTO

Irina Nork

Tabletop Exercises (TTX)

Your company falls victim to a cyberattack. Cybercriminals hack into servers, encrypt data, and publish sensitive data on the dark web. The incident becomes public. Customers expect explanations. The attacker demands money.

Do your incident response plans work? Have you tested your emergency plan under realistic conditions?

What are Tabletop-Exercises (TTX)?

- **Customized, interactive cyber incident simulations**—your team is placed inside realistic cyber incident scenarios, guided by experts, challenged by real-time decisions, and trained to respond confidently under pressure. It's hands-on, engaging, and tailored to your organization.
- **Realistic stress situations in a safe environment**—we test your preparations, communication, and response coordination in a secure and regulated environment, comparable to a digital "military drill." Teams feel the intensity of a real attack, but without the real-world risk.
- **Clarity and resilience**—we help you identify what works, uncover blind spots, and refine your defense strategy. The result: a clearer plan, a well-coordinated team, and a company that's genuinely ready for the next cyber crisis.

Why AwareTec?

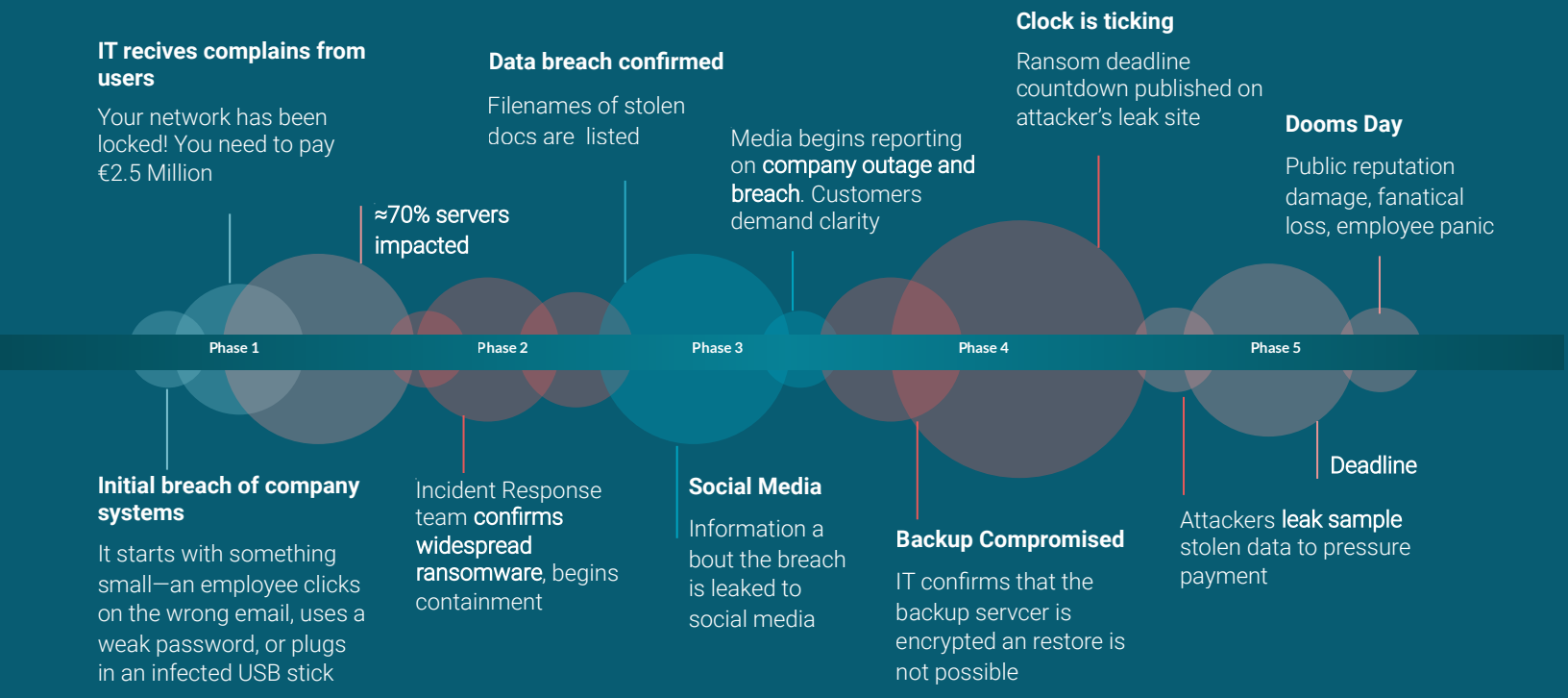
- **Proven expertise**—work with world-class experts who have strategic and hands-on experience defending critical infrastructure and managing real incidents. Our experts don't just talk theory; they've lived it.
- **Tailored for every level**—our tabletop exercises bring together both technical teams and executive leadership. We help IT and OT professionals and management align on strategy, communication, and compliance when it matters most and under pressure.
- **Clear and actionable results**—you'll walk away with clear, prioritized recommendations and a practical roadmap to strengthen your team, processes, and preparedness. Concrete steps that make your organization more resilient.

From Cyber Incident to Crisis

Why is Preparation Essential During the Escalation of an Attack?

A cyberattack can escalate quickly—from a single click to a full-blown crisis involving data leaks, downtime, and reputational damage.

This highlights why preparation and coordinated response at all levels are crucial.



Initial breach of company systems

It starts with something small—an employee clicks on the wrong email, uses a weak password, or plugs in an infected USB stick

IT recives complains from users

Your network has been locked! You need to pay €2.5 Million

≈70% servers impacted

Incident Response team **confirms widespread ransomware**, begins containment

Data breach confirmed

Filenames of stolen docs are listed

Social Media

Information a bout the breach is leaked to social media

Media begins reporting on **company outage and breach**. Customers demand clarity

Backup Compromised

IT confirms that the backup servcer is encrypted an restore is not possible

Clock is ticking

Ransom deadline countdown published on attacker's leak site

Attackers **leak sample** stolen data to pressure payment

Dooms Day

Public reputation damage, fanatical loss, employee panic

Deadline

Tabletop Exercises in Action

Why tabletops are important: Turning Uncertainty into Cyber Preparedness

Strategic Results

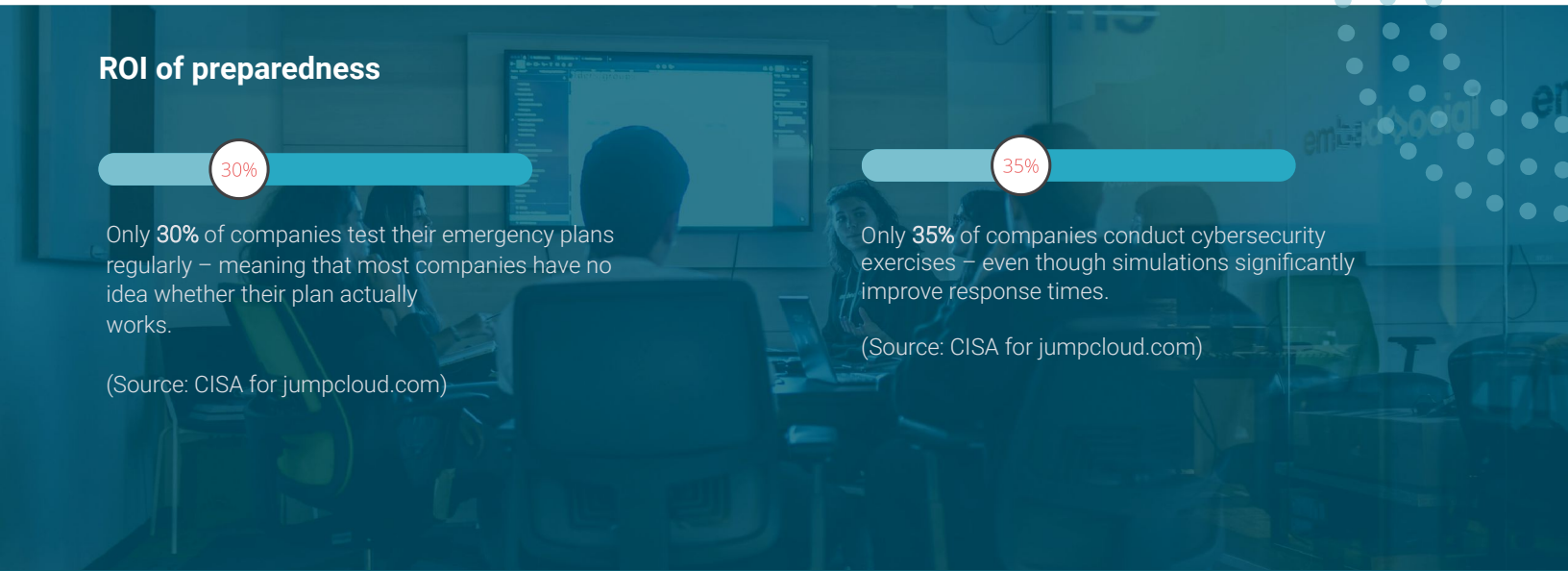
- Build awareness among executives about cyber risks and how to respond effectively
- Test and refine decision-making under realistic crisis conditions
- Align cybersecurity initiatives with business strategy to strengthen overall resilience

Response Capabilities

- Strengthen communication and teamwork between IT, OT, and leadership
- Reveal hidden vulnerabilities, weak points, and escalation delays in a safe environment
- Experience real-world attack scenarios in a guided, hands-on format

Measurable Improvment

- Validate crisis response and recovery plans with realistic simulations
- Receive clear, actionable findings and structured reports
- Increase team coordination, speed, and clarity when it matters most



ROI of preparedness

30%

Only **30%** of companies test their emergency plans regularly – meaning that most companies have no idea whether their plan actually works.

(Source: CISA for jumpcloud.com)

35%

Only **35%** of companies conduct cybersecurity exercises – even though simulations significantly improve response times.

(Source: CISA for jumpcloud.com)

Tabletop Exercises

Formats

Our exercises are designed both for IT and OT environments.

We offer the following TTX formats:

Discussion-Based

Create clarity before a crisis hits

Many organizations have incident response plans, but in practice employees are often unsure about their responsibilities when an attack occurs. This leads to delays and confusion.

Your advantage:
Through a guided discussion, teams align on roles, decision-making processes, and escalation paths. Everyone knows what to do, when to act, and who is responsible. The result is a faster, coordinated response when it truly matters.

Scenario-Based

Build confidence through realistic cyber attack simulations

Attacks like ransomware or data breaches are complex, and teams rarely experience the full progression of such incidents.

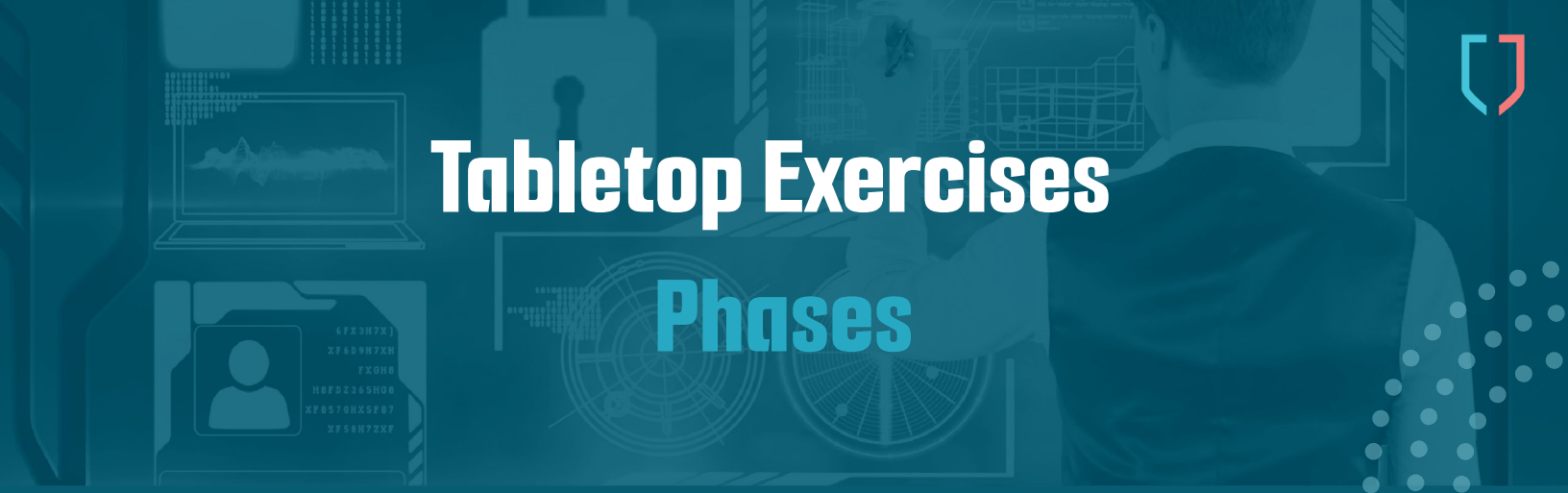
Your advantage:
By walking through a realistic scenario, participants understand how an attack unfolds, how it impacts the business, and what actions to take at each stage. This strengthens decision-making and builds confidence in managing high-risk situations.

Practical Response Exercise (Functional and Technical)

Train like it is real

In many incidents, IT, OT, security teams, and management work in silos, leading to mistakes and delays. Technical teams often realize too late that processes are not functioning as expected.

Your advantage:
This exercise simulates a live cyber incident where teams must detect, contain, communicate, and recover together. It strengthens cross-departmental collaboration, validates processes, and reinforces the technical foundations of your incident response.



Tabletop Exercises

Phases

From goal setting to evaluation—a structured roadmap for realistic and effective cyber incident simulations

Goals and Objectives

- Define the scope
- Decide on participants
- Decide an escalation level
- Set goals taking into account:
  - Vulnerability
  - Organizational priorities
  - Existing processes
  - Security measures

Scenario Types and Methods

- Identify the scenario type based on:
  - Contingency plans
  - Specific cyberattack
  - Threat landscape
- Decide on a delivery method
  - Discussion-based
  - Scenario-based
  - Functional and technical

Tabletop Exercises Design

- Research:
  - Based on the attack surface
  - Based on the company's risk matrix
- Create a storyline for the tabletop exercise
- Integrate escalations
- Create player manuals (video or presentation)

Injections

- Design and produce injections
- Provide new updates during the exercise:
  - Include relevant information
  - Provide realistic experiences
  - Base on escalation level

TTX-Execution

- Setting up the venue for the meeting
- Moderating the exercise
- Escalation
- Documenting the results

Evaluation and Improvements

- Analysis of the effectiveness of the tabletop exercise:
  - Technology
  - People
  - Processes
- Identification of opportunities for improvement
- Development of the draft after-action report (AAR)

Tabletop Exercises

Strategic Considerations

To ensure that a tabletop exercise is not just a means to an end but also has a real impact, several key factors must be taken into account.
The aim is to gain practical insights, strengthen confidence in one's actions, and identify critical weaknesses at an early stage.

Goals and Scope—Focus Drives Results

- **Clear objectives**—do you want to test emergency procedures, evaluate decision-making under pressure, or review communication workflows?
- **Realistic scope**—we adjust the duration, number of participants, and level of complexity to match your maturity and resources.

Scenario Design—Realistic, Not Theoretical

- **Individual & realistic scenarios**—tailored scenarios based on your current threat landscape and business processes. This feature ensures relevance and helps uncover real risks.
- **Escalation**—you choose the level of intensity, whether it starts with a minor IT disruption or develops into a full-scale corporate crisis.

Stakeholders—Stronger Teams, Better Outcomes

- **All critical areas are included**—IT and security teams, management, communications, legal, HR, and business units. Every perspective counts.
- **Decision-makers and operational teams**—everyone collaborates directly, enabling realistic, informed dialogue and faster coordination during real incidents.

Execution, Engagement, and Logistics

- **Delivery**—fits your needs, whether on-site, remote, or hybrid.
- **Experience**—interactive moderation keeps participants engaged and focused.
- **Implementation**—we use structured methods, visuals, and operational triggers to ensure professional execution and measurable outcomes.

Tabletop Exercises

the Process

Most companies rightly consider traditional tabletop exercises to be very labor-intensive. At AwareTec, the opposite is true: we take on the bulk of the work, analyzing, developing the scenario, moderating the exercise, and finally delivering clear results and recommendations.

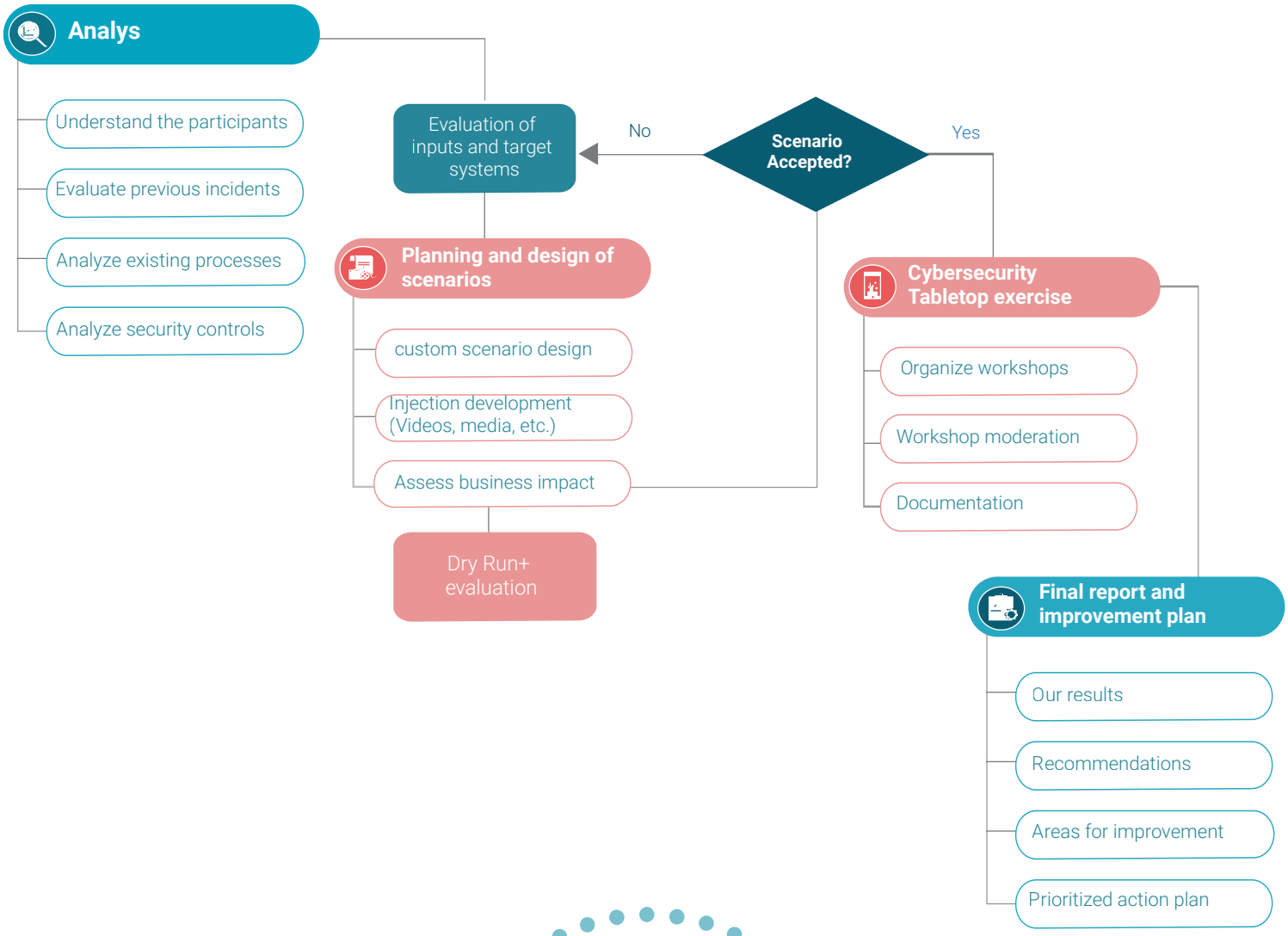
For you, this means minimal time investment with maximum benefit. Your teams invest only a few hours, but you get realistic insights, clear recommendations, and greater certainty.

A clear roadmap – from defining goals to implementation and improvement

Tabletop Exercises

Scenario Design

Every tabletop exercise is based on a customized scenario. To ensure that it is realistic, relevant, and effective, we follow a clear process.
We offer you an exercise tailored precisely to your company, giving you real confidence in your ability to respond effectively.



Tabletop Exercise

Your Benefit

How Our Cyber Crisis Exercises Deliver Real Value?

Strategic Planning and Alignment

We start by understanding what matters most to your organization. This includes your critical assets, key business processes, and existing documentation such as backup, business continuity, and incident response plans. With this foundation, we design exercises that are **realistic, relevant, and fully aligned with your environment**.

Scenarios Tailored to Your Risk Landscape

We build our cyber incident scenarios around your specific threat profile. They can gradually increase in complexity to challenge your teams and test their ability to make decisions under pressure. Each scenario evaluates how well your organization can respond **in line with your emergency procedures and security policies**.

Expert Facilitation and Real-Time Feedback

Our specialists guide your team through the exercise in a structured and engaging format. Participants receive contextual updates, realistic developments, and direct feedback during the scenario. This approach encourages **meaningful discussions and realistic decision-making.**

Actionable Insights and a Comprehensive Report

After the exercise, you receive a clear and detailed report. It measures your performance against internal standards and industry best practices. The report highlights strengths, pinpoints weaknesses, and provides **prioritized recommendations to improve your incident response capabilities**.

Tabletop Exercises

Work Package

Our cyber tabletop exercises (TTX) are designed to strengthen the resilience of organizations, improve decision-making, and prepare teams to effectively manage cyber incidents.

The work package includes the following:

- Tabletop Exercises / Simulated Cyber Crisis
- Realistic scenario tailored to your company
- Expert moderation and guided discussion
- Detailed report on the assessment of readiness
- Roadmap to optimization, prioritized and risk-based

Optional Extensions:

- Cyber Threat Intelligence - Analysis of your external attack surface and simulation based on real attack vectors and threat information
- Technical exercise - Practical simulations for IT/OT, SOC, and incident response teams
- Hack your plan—gap analysis and actionable improvements, a scenario that specifically exploits your known vulnerabilities
- AR experience - Crisis management gamification with AR glasses

Get In Touch

E-Mail: mail@awaretec.de
Website: www.awaretec.de

OR

Make an appointment