Cyberpsychologist Assisted Wargaming & Crisis Management

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **1 Gün**

Overview

Traditional cyber security awareness training solutions focus mostly on delivering generic, computer based, 'one size fits all' courses to address the human component of risk at organisations. The CyberFish Company introduces novel methodologies by blending employee awareness with personalised talent management solutions in order to strengthen the individual defences of employees and improve corporate incident response capabilities.

Our innovative approach and cyberpsychology cycle directly leverages on cutting edge research within the area of digital behaviours and by addressing the human component of cyber security risk on several levels of the organisation, ultimately leading to a transformed security posture and an effectively functioning cyber security team.

In our scenario driven, interactive workshop (3hr event & 1hr washup) we challenge participants to work together as a team and experiment with different cyber crisis scenarios.

Together with the technical learnings to be taken away from the workshop we will also help understand and address the current strengths and development areas in your team dynamics: how different individuals have opportunities to improve the way they communicate, interpret complex situations, make decisions and cope with stress in a mission critical setting.

Testimonials:

"Your wargame event helped me discern the multiple layers of the problem relating to the complexity of managing stakeholder interests in a mission critical situation."

"Great intellectual simulation of the case study of a cyber attack."

"I found The CyberFish wargame simulation a fun and hands-on way to learn about possible cybersecurity threat scenarios and experiment with how I would respond."

"Your wargame event helped me discern the multiple layers of the problem relating to the complexity of managing stakeholder interests in a mission critical situation."

"The event was really quite fun and I see a massive potential for it to be used as a tool for companies to understand what additional training and resources they need to cope better with a cyber security incident."

Prerequisites

No technical experience is required to participate. From an industry perspective, this simulation is based on an attack based in a neutral office setting. This is a tabletop exercise. Existing teams are encouraged to apply, but we welcome individual players as well. We do have tailored cyber crisis scenarios for most industry environments, enquire for more detail.

What You Will Learn

Our interactive exercises help decision makers to:

- Test the effectiveness and the overall posture and functioning of the leadership team in case of a crisis situation
- Assess the capacity of the incident/crisis management team to provide appropriate situational awareness to the different stakeholders and audiences within one hour from detecting a breach
- Expose and address weaknesses and development areas in team dynamics, communications and decision making
- Assess the incident/crisis management team's readiness to implement a range of proper recovery and communication procedures in the event of a data breach and as such contribute to incident response planning
- Enhance cyber and data protection awareness, readiness and team synergies in the event of an incident and or crisis
- Develop individual development plans and corporate contingency plans for addressing crisis management

Benefits

- Participants will be able to compare their actual response to different data breach scenarios and the expected response by the facilitators.

Participants can thus learn from technical cyber security, data protection, public relations and behavioural experts the best demonstrated practice and decision making milestones for data breach incidents.
- Cyberpsychologist facilitators will identify and report gaps in training and individual competencies that will allow participants to work through threat scenarios together as a team and experiment their ability to cope with mission critical situations both from a technical and behavioural perspective.
- Organisations can improve their organisational defences by understanding their leadership team's reactions and facilitate their understanding of how they can perform under pressure, coping with stress and negative emotions as a team.

Outline

The CyberFish Behaviourist Assisted Wargaming Exercises allow teams get to experiment with different scenarios and see how they would react in a hypothetical incident situation. Assess critical competencies that are needed when mitigating a mission critical incident situation. Cyberpsychologists assist the tabletop exercise and make observations on the behaviour of the participants with a view to prepare a detailed report to be used in the further development of employees. The report elaborates employee behaviours from the perspective of the CyberFish Responsible Cyber Behaviours Framework© and provides individual risk exposure together with specific mitigation paths for each employee. Our tabletop simulation exercises are run either at QA's CyberLabs at International House, St Katherine's Docks in London, or in house at our clients' premises.

Based on the individuals performance on the simulation exercise and the CAA assessment, the following descriptive reports will be prepared detailing the outcomes:

1. Team Group Dynamics Report, elaborating on:

- An executive summary for the attention of the Incident Management/Crisis Management Team based on the overall team dynamics and performance (anonymised for all participants)
- A team heat map based on human error exposure and strengths
- Potential risks and impacts from the identified individual error areas and learning and coaching opportunities for the identified strength areas
- Observations with regards to team behaviour and performance
- Other topics depending on team results and specific target areas

2. Individual Reports, elaborating on:

- The CyberFish Responsible Cyber Behaviours Framework© and definitions
- An individual heat map of cyber risk exposure
- Individual results and comments following the 6 different elements of the CyberFish Responsible Cyber Behaviours Framework©
- Best practices to eliminate or reduce actual risks

In addition to the post event reports both team and individual face to face feedback sessions (1hr) with a cyberpsychologist are available, to discuss and reflect on the outcomes and explore personal strategies to mitigate exposure and exploit strength areas.