



Cyber Crime Dinner

PwC Cyber Awareness Training



Description

The Cyber Crime Dinner “Diagnosis: Extortion – Hunting for Clues Between Servers and Scalpels” is an interactive dinner game designed to build cyber security awareness in an engaging and memorable way.

Storyline & Scenario

The scenario takes place in the fictional Lichtenwald Hospital, which has fallen victim to a devastating cyber attack. All systems have been encrypted by ransomware and operations have come to a standstill. Participants take on different roles – from the hospital director and the senior physician through to the head of IT and an attentive patient – and must work together to reconstruct what happened, uncover the attacker’s motive and find out whether an insider or the attacker is among them. The storyline is based on real cyber incidents and draws on authentic attack methods such as social engineering, phishing, ransomware and AI-supported techniques.

Learning Objectives

Through the Cyber Crime Dinner, participants develop a comprehensive understanding of modern cyber threats, the impact of internal friction points on IT security and effective protective measures. The following aspects are addressed:

- Physical security: Tailgating
- The principle of “least privilege”
- Risks posed by publicly accessible sensitive information
- Psychological triggers / social engineering
- Recognizing phishing e-mails
- The importance of a healthy error culture
- Ransomware attacks
- Backups and recovery procedures
- The importance of thorough preparation and emergency exercises

The individual topics can be explored in greater depth in a workshop following the game. A reflection session on the content allows targeted knowledge to be introduced and specific anchor points from the game to be addressed.

Materials

The game consists of the following materials (either already printed or provided digitally as a PDF, depending on the variant selected):

- 9 character booklets — one booklet per participant, each with an individual role description, personal background, relationships with other characters as well as sealed sections containing clues that are revealed step by step as the game progresses.
- Event booklet / facilitation guide — contains the prologue, round-by-round event narratives, facilitation instructions with timings as well as the full solution to the case.
- Additional information document (“Shadow wiki”)— with background information and technical explanations of cyber security concepts (social engineering, ransomware, phishing, deepfakes) and a glossary of key terms.
- Supplementary materials — such as e-mails, system log extracts and further in-game documents that serve as clues.
- Name badges, voting slips.

Security Awareness – An Immersive Learning Experience with Lasting Impact

The game offers an immersive, scenario-based introduction to real cyber threats such as social engineering, phishing and ransomware. By experiencing an attack scenario first-hand, participants develop a deeper understanding of cyber risks and protective measures.

- **Hands-on experience:** By actively experiencing a realistic attack scenario, employees learn intuitively and emotionally – this leads to better risk awareness than a standard training course
- **Broad target group:** From employees to executive level – the game makes cyber threats understandable for every position and also highlights the challenges at the various levels
- **Authentic scenarios:** Based on real attack methods (social engineering, phishing, AI-supported attacks) – instead of theoretical examples
- **Organizational resilience:** Teams jointly develop a deeper understanding of cyber risks and learn to manage and avoid crisis situations more effectively
- **Compliance & governance:** Documentable awareness training that directly addresses the increasing regulatory requirements calling for regular employee awareness measures (e.g. NIS-2, ISO 27001 & BSI IT-Grundschutz)

Why the Cyber Crime Dinner?

State-of-the-art cyber security awareness: The storyline of the game is based on authentic, real-world attack methods – including AI-supported attacks and social engineering techniques – and therefore reflects the current cyber threat landscape.

Easy to run and a low-barrier introduction to the topic: The Cyber Crime Dinner requires little technical prior knowledge from participants. The game format introduces complex cyber security topics naturally through storytelling and role play, making them accessible and appealing for every target group. Delivery is straightforward thanks to ready-to-use game materials and a clearly structured facilitation guide.

Event-based awareness: Security awareness simulations are usually implemented with the help of technology (iPad/computer), immersing participants in cyber attack and defense scenarios. While PwC products such as „Game of Threats¹“ or the „Cyber Escape Room²“ are technology-driven and focus on decision-making within a digital interface, the Cyber Crime Dinner differentiates itself through its analogue, social and narrative-driven format – with an emphasis on personal interaction, team discussion and an immersive (dinner) experience. The two products complement each other: Game of Threats covers the area of digital simulation, while the Cyber Crime Dinner closes the gap for personal, event-based awareness experiences.

Product Variants & Pricing

Variant	Description	Price
Digital materials (DE/EN)	One complete game set, delivered in digital form. Can be used multiple times. Ready to use.	2.500 €
Print materials (DE/EN)	One complete game set, delivered in printed form (incl. packaging). Ready to use. From 5+ sets: volume discount (10%).	250 € / Set Incl. shipping cost
Event – at PwC	Facilitation & delivery of the Cyber Crime Dinner at a PwC office/restaurant, 5–36 people per event Print materials are included.	4.000 - 9.500 € / Event

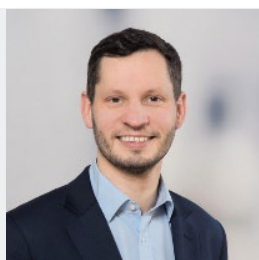
¹ <https://www.pwc.de/de/cyber-security/game-of-threats.html>

² <https://www.pwc.de/de/cyber-security/information-security-management/innovatives-trainingstool-der-cyber-escape-room.html>

Event – at your premises	On-site facilitation, preparation, delivery, follow-up (game + subsequent workshop/reflection), 5–36 people per event Print materials are included.	6.000 – 11.500 € / Event
Virtual event	Facilitation in an online session (e.g. via Teams), preparation, delivery, follow-up, 5–36 people per event Digital materials are included.	3.500 – 8.000 € / Event
Customization	Scenario adapted to your industry or specific topics.	On request

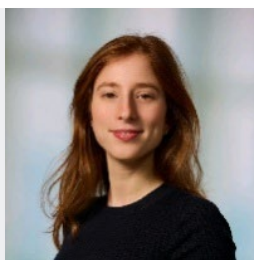
Your Contacts

Feel free to get in touch with us!



Thomas Klir

+49 (0) 171 2852714
thomas.klir@pwc.com



Lena T. Schramm

+49 (0) 171 6422902
lena.theodora.schramm@pwc.com