

TRACK 1 · TRADECRAFT

Executive Ransomware Simulation

Lead your organisation through a ransomware crisis before one finds you

DURATION	FORMAT	SKILL	MAX	COURSE LEAD
1 day	Workshop and Simulations	Beginner no tech-expertise needed	12 students	Redacted

Ransomware is a leadership test. Be ready to lead when the pressure is on. If ransomware disrupted your organisation tomorrow, could your leadership team make the right decisions? Test your readiness before a real crisis puts continuity, reputation and stakeholder trust at risk.

Step into an escalating ransomware scenario, built specifically around your sector and risk profile and based on real-world cases from Responders.NOW in collaboration with Birdwatcher Group. Face operational disruption, ransom demands, threatened data leaks and media scrutiny.

Aims to bring together board members, executives and leaders from IT, security, finance, legal and communications. Practice making decisions with incomplete information, while attacker tactics and business impacts are explained in plain English.

TARGET AUDIENCE

- Security officers,
- CISOs, privacy officers,
- CEOs,
- CFOs,
- General counsel,
- Crisis communications leads,
- Risk and compliance officers,
- Board members and senior executives with accountability for organisational resilience.

PRICING

Individual	€1,499 / seat (Ex-VAT)
Custom	Custom pricing on request

Custom covers bespoke in-house delivery for companies and teams, adapted to your threat environment.

→ **Practical component:** A 4-hour escalating ransomware simulation built on real-world cases. Teams face operational disruption, ransom demands, data leak threats and media scrutiny — and must make decisions with incomplete information throughout.

→ **Individual vs Custom difference:** Individual option uses a scenario built around a representative organisation in a realistic but generic context. The Custom option shapes the scenario to your actual sector, risk profile and stakeholder landscape.

LEARNING OBJECTIVES

- Understand the ransomware threat landscape and attacker playbook
- Clarify leadership roles, responsibilities and decision-making priorities
- Practise crisis communications under time pressure
- Navigate ransom demands and negotiation dynamics
- Understand NIS2 obligations and regulatory reporting timelines
- Test teamwork, escalation and cross-functional coordination
- Expose gaps in your incident response plan
- Leave with actionable improvements

SCHEDULE

Day 1

MORNING SESSION

- Workshop introduction and objectives
- The ransomware landscape: how attacks unfold and why leadership decisions matters
- Anatomy of a modern ransomware incident: timeline, stages, attacker playbook
- Ransom demands, negotiation dynamics and double extortion
- NIS2 obligations: what you must do, report, and when
- Stakeholder management under pressure: board, regulators, media and customers

— *Lunch break* —

AFTERNOON SESSION

- Scenario briefing and team role assignment
- Phase 1: Discovery — the attack is detected; first-hour decisions
- Phase 2: Escalation — ransom demand received, systems offline, regulatory clock starts
- Phase 3: Dilemma points — data leak threat, media enquiry, board call
- Phase 4: Resolution — negotiation outcome, communications, recovery
- Full debrief: decisions reviewed, gaps identified, improvements agreed

WHAT YOU TAKE HOME

- Field Dossier — printed handbook of every lesson, framework and case study
- Cheat Sheets — ransomware response checklist and decision framework
- Granted Access — real world practitioners from Birdwatcher Group and its network
- Tradecraft Toolkit — incident response templates and NIS2 reference guide
- After Care — up to 6 months of direct email access to your course lead

Register for this course now!

Email us at: trainings@birdwatchergroup.com OR fill in the form on our website: www.birdwatchergroup.com/intelligence-nest