CyberOne

Cyber Incident Tabletop Excercising

G-Cloud 15

Pricing Card

Cyber Incident Tabletop Exercising

Run The Drill. Create The Confidence. Build The Resilience.

Turning Plans into Proven Readiness

Tabletop Exercising is a guided, scenario-based workshop that brings your key stakeholders together to test your organisation's ability to respond to a cyber incident.

Rather than a technical drill, it focuses on decision-making, communication, escalation and collaboration across leadership, IT, legal, compliance and operations. These sessions help you validate your incident response plan, uncover hidden weaknesses and build confidence at board level.

Why Tabletops Matter

Cyber incidents rarely happen on your terms. Tabletop Exercising ensures your teams are ready, aligned and confident to respond when it matters most.

- **Incidents Are Inevitable –** Ransomware, insider threats, supply chain compromise and data exfiltration are everyday realities.
- **Plans Must Be Tested –** Tabletop exercises stress-test response procedures in a safe environment.
- **Regulators & Insurers Expect it** – Regular exercising demonstrates preparedness, supports compliance and strengthens your cyber insurance risk profile.
- **Boards Demand Assurance** – Resilience must be evidenced, not assumed.

Turning Practice Into Progress

Every exercise is designed to leave you stronger than before, translating rehearsal into real improvements that enhance preparedness, confidence and resilience.

Tailored Scenarios
Realistic threats designed for your industry and risk profile.

Executive Engagement
Active participation from leadership and operations.

Actionable Findings
Clear, practical report with prioritised recommendations.

Expert Facilitation
Led by CyberOne consultants to guide and challenge teams.

Dynamic Injects
Real-time twists to test decision-making and escalation paths.

Role-Based Access Control
Defined steps to strengthen preparedness and confidence.

The Cyber Incident Exercise Lifecycle

A tabletop exercise isn't a one-off event, it's a structured journey. Our lifecycle ensures every step, from planning to debrief, delivers practical lessons and measurable improvements that strengthen organisational resilience.

1. Scope

Understand business, define objectives, stakeholders and scenarios to ensure the exercise reflects real business risks.

2. Design

Develop realistic and relevant scenarios that align with regulatory, operational and threat contexts.

3. Run

Facilitated simulations with realistic injects from ransom notes to regulator calls under pressure.

4. Debrief

Capture of lessons immediately, highlighting key decisions, strengths and areas for improvement.

5. Remediate

Turn findings into a prioritised action plan mapped to risks and regulatory expectations.

6. Re-Test

Turn findings into a prioritised action plan mapped to risks and regulatory expectations.

Why Choose CyberOne?

We don't just run Cyber Incident Tabletop Exercises. We bring the weight of real-world credentials, deep cyber expertise and regulator-ready outcomes to every engagement.

CREST & NCSC Pedigree

Delivered by CREST-approved practitioners and aligned to NCSC guidance, giving regulator-grade assurance.

Sector-Specific Scenarios

Realistic, highly relevant exercises shaped around the risks, pressures and evolving regulations of your industry.

Third-Party Supply Chain Scenarios

Incorporating supplier compromise and third-party fallout, now a baseline regulatory expectation.

Proven Incident Response Experience

Led by NCSC CIR (Standard Level) and CREST-approved responders with decades of frontline breach expertise.

Board-Ready Outcomes

Strategic, plain-language insights that equip boards with confidence and clarity.

End-to-End Cyber Security Portfolio

From Consulting, Professional to Managed Services a complete pathway to resilience.

General Pricing Information

No sector-specific pricing applies. The quoted pricing information for this service applies equally across all client sectors.

All pricing information is quoted in pounds sterling (GBP) and prices are exclusive of VAT at the applicable rate (unless otherwise stated)

Resource-Based Pricing (Time & Materials)

Resource-based pricing is defined in the SFIA Rate Card for this service.

The SFIA Rate Card (available as a separate attachment, downloadable from the service web page) lists the options of day rates applicable to this service, for each SFIA grade, with the bold figure showing a typical average for a London based service delivery before any discounts are applied.

Buyers and suppliers will explore the relevant rates in clarification questions permitted as part of the buying process and agree as part of a Call-Off Contract.

Education Discounts

Additional discounts may apply to educational institutions across all charging models and will be negotiated during the purchasing stage.

Fixed Price Service Charge

Where applicable, services can be provided on a fixed price basis. For example, using an assumed number of resources at the agreed SFIA rate, with an agreed set of deliverables.

This approach enables accurate spend control and forecasting for customers and can be negotiated during the purchasing stage.

Volume / Combination Discounts

All prices are quoted without volume or combination discounts. Discounts may apply where the volume or work combination is appropriate, but will be subject to negotiation and agreement during the purchasing stage.

Pricing for Combined Services

If a client wishes to purchase several discrete G-Cloud 15 services as a single package, the total price will be the combination of the individual service line prices.

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.

CyberOne

hello@cyberone.security

+44 (0) 3452 757575

cyberone.security