CyberOne

Cyber Incident Tabletop Exercising

G-Cloud 15

Service Description

Service Description
Cyber Incident Tabletop Exercising

To respond effectively to Cyber Incidents, CyberOne proposes a tailored Cyber Incident Exercising simulation designed to simulate a real-world ransomware attack and to practice response strategies in a controlled environment. The participants will be selected in advance, it is likely to be a selection from leadership and communication teams, emergency preparedness and area managers or hospital managers.

The primary objective of this exercise is to enhance the organisation's participants' knowledge, readiness and resilience against ransomware attacks. By participating in this simulation, the selected team will gain valuable insights into the complexities of ransomware incidents and the critical decisions required to mitigate their impact – including media coverage. It will therefore also create valuable insights and informative educational content that will enhance the executive team's knowledge around responding to cyber events.

Following the exercise, we will provide a comprehensive documentation write-up, including key observations, identified gaps and actionable recommendations to strengthen your incident response, Disaster Recovery and BCP capabilities.

Methodology
Our Approach to Cyber Incident Tabletop Exercising

Pre-Exercise Preparation

CyberOne will work closely to prepare a realistic and tailored ransomware scenario. This will include:

- Developing and customising scenario materials that reflect threats relevant to the operational and technical environment.
- CyberOne will review the Incident Response and Business Continuity Plan, which also lists the key people and their Roles & Responsibilities.
- Distributing the IR plan and relevant scenario context to designated participants and CyberOne facilitators.
- Scheduling the exercise session in coordination with selected participants and CyberOne's facilitators.

Cyber Incident Tabletop Exercising

Purpose: To provide a walk-through of a realistic, scenario-driven Cyber Incident Tabletop Exercise where the Participants can collectively practise decision-making under simulated pressure without fear of failure or embarrassment.

CyberOne

Format:

- A facilitated workshop
- Scenario focused on a cyber incident with business-wide impact (ransomware, operational disruption, reputational risk)
- Facilitated group discussion at each inject phase, highlighting key decision points
- Realistic time-pressured decision-making injects
- Inclusion of cross-functional role challenges

Core Focus Areas:

- Command and control structure clarification
- Executive decision-making alignment
- Communication and media response management
- Regulatory and legal obligations
- Financial and operational impact assessment
- Internal stakeholder management

Deliverables:

- Customised, organisation-specific exercise scenario and inject script
- Facilitation by a senior consultant
- Live exercise play with tailored role prompts
- Real-time observations and facilitator feedback
- Post-exercise summary report with key observations, lessons learned, and actionable recommendations
- Recommendations for future maturity steps (e.g., further technical drills, playbook updates, policy refinements)

The Exercise

The National Cyber Security Centre (NCSC) recommends Cyber Exercising as a way to ensure that effective responses to potential issues are identified early. This scheme offers valuable tools and resources that can be leveraged to enhance the effectiveness of ransomware tabletop exercises, ultimately helping organisations better prepare for and respond to cyber-related disruptions.

Define What to Exercise
CyberOne will work with your team to define the correct areas for exercising

Secure Senior Level Endorsement
Your team will be chosen from those who have the power to make decisions regarding the potential cyber disruptions

Select The Most Effective Approach
Our expertise with providing exercises of this nature has proven our approach which is inclusive and challenging

Create Team & Agree Participants
We will provide a highly experiences & personable team to assist with the exercising

Create & Agree Metrics
Our approach ensures that metrics for success are defined and agreed before commencing exercises

Create & Develop Exercise Scenarios
Our team will work with you to develop realistic scenarios that will test your response plans

Create & Develop the Exercise Injects
Exercise injects will be realistic and interactive

Develop Guidance for Participants
Scenarios will be drawn and improved from existing cyber related disruptions

Run the Exercise
Independent legal counsel will be provided to assist with providing experience & guidance throughout the exercises. Separation from existing legal counsel will ensure an independent viewpoint.

CyberOne

Facilitation of the Exercise

The Cyber Incident Tabletop Exercise will be delivered in a structured and interactive format, designed to test real-time decision-making and response coordination:

- Introduce the scope, objectives, and scenario of the exercise to all participants.
- Guide the response team through the initiation of the IR plan, with emphasis on detection, containment, communication, and recovery processes.
- Facilitate real-time discussion and critical decision-making to test organisational resilience and process maturity.
- Dynamically adapt the scenario in response to participant actions to simulate realistic challenges and pivot points.

Debrief and Feedback Collection

As the final step of the ransomware exercise, CyberOne will facilitate a conversation where the participants will discuss observed strengths and any procedural or communication gaps.

Documentation and Reporting

CyberOne will present a post-exercise report remotely, including a "lessons learned" summary highlighting key findings and recommendations for enhancing the IR plan.

Commercial Overview

By choosing CyberOne to conduct a Cyber Incident Tabletop Exercise, the following can be expected:

- Enhanced Preparedness: Equip the selected participants with the knowledge and skills needed to respond swiftly and effectively to ransomware attacks.
- Improved Co-ordination: Foster collaboration and communication among key stakeholders during a crisis.
- Reputation Management: Strengthen your organisation's ability to protect its reputation by demonstrating a proactive approach to cyber security.

Our recommendation would be to facilitate this as a face-to-face exercise, enabling participants to fully engage together as they progress. The initial simulation exercise can sometimes be a new experience, and once the first session has been completed any further exercises can be completed remotely with more ease. The pricing option below is for either a remote or face-to-face exercise.

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.

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