RED GOAT
CYBER SECURITY

CYBER CRISIS EXERCISE

IMMERSIVE, THREAT-LED CYBER CRISIS EXERCISES TO EVALUATE AND DEVELOP YOUR LEVELS OF PREPAREDNESS, RESPONSE AND RECOVERY.

KEY BENEFITS

BOOST SKILLS
Exercises improve teamwork, confidence and make members more aware of their individual roles and responsibilities in a realistic crisis scenario.

IDENTIFY OPPORTUNITIES TO IMPROVE
Evaluate what is working well and where resilience can be improved.

TEST INCIDENT RESPONSE PLANS
Improve response plans and playbooks. You may decide you need specific playbooks for the most likely attacks for instance ransomware. It also allows you to test your command structure and escalation processes.

DEMONSTRATE COMPLIANCE
Demonstrate preparedness to regulatory bodies through documented exercises and lessons learned, thereby ensuring alignment with compliance requirements.

Overview

A tabletop exercise simulates cyber attacks to test response plans, focusing on human and procedural aspects rather than technical defences. It identifies weaknesses, enhancing cyber resilience by refining skills in a realistic setting.
Exercises feature evolving scenarios and end with a debrief and recommendations for improvement, tailored to organisational assets and risks.

Why Businesses Choose Red Goat

We have extensive experience of running exercises within a wide range of often regulated industries. These include financial services, law, cloud computing, SaaS, and NGOs.
This broad experience, combined with our expertise and knowledge, ensures you get the most out of your cyber tabletop exercise.

We work in partnership with your team to develop a bespoke exercise as well as being able to provide training, plans and playbook assessments and a report.

CYBER CRISIS EXERCISE

WHAT'S INCLUDED:

FULLY MANAGED EXERCISE
We work with you to plan and deliver a high quality, bespoke cyber-attack exercise. This includes a full run-through prior to the exercise.

POST-EXERCISE HOT DEBRIEF
After the exercise we run a short debrief. This reviews key findings, lessons learned, and collects participant feedback for inclusion in the report.

AFTER ACTION REPORT
We deliver a full report and executive summary on how the exercise met the objectives of the exercise. This includes lessons learned and prioritised recommendations.

CYBER EXERCISE DESIGN STAGES

5 STEPS TOWARD INCREASED RESILIENCE

SCOPING
We begin by assessing your current plans and playbooks and ensuring we have a full and rounded understanding of your important business services, data and organisational maturity. We then work with you to set the key objectives for the exercise.

SCENARIO DEVELOPMENT
We work with your team to craft a realistic, engaging, and challenging cyber incident simulation. We develop a range of multi-media and additional components to boost realism and immerse attendees in the experience.

RUN-THROUGH
A complete run through is scheduled before the exercise for you and everyone involved in the development process. We go through the entire exercise as it will happen on the day.

EXERCISE
One of our senior consultants will deliver the entire exercise, either virtually or in person. We run a hot debrief after the exercise to capture all the ideas and recommendations generated by the exercise and from participants.

REPORTING
You will receive a full written report with recommendations for improving your level of preparedness. Use this to improve resilience and demonstrate compliance to regulators and third parties.

Contact Us

Email: info@red-goat.com
Website: red-goat.com
Phone: +44 117 325 9190
Address: Red Goat Cyber Security LLP, 470 Bath Road, Bristol, BS4 3AP

RED GOAT
CYBER SECURITY