Privia SECURITY

Cyber Exercise Service

Professional Defensive Security Services

"No Success on an Unprepared Front!"

The information contained in this document pertains to the Defensive Services performed by Privia Security Information Technology and Consultancy Services Inc. and is of a **general** nature. All information in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

"Cyber Security Exercises enable teams to gain experience through realistic scenarios, allowing for quick and effective responses in times of crisis."

Today, cyberspace is recognized in literature as the fifth domain of warfare—after land, air, sea and space. Governments' and organizations' awareness of the potential consequences of cyber threats continues to grow every day, with the goal of detecting and neutralizing risks effectively. The most effective actions for detecting threats in cyberspace are cyber exercise processes based on realistic scenarios and evolving conditions.

Cyber Security Exercises are active/passive simulations based on scenarios that an organization organizes to test its cybersecurity measures and crisis management capabilities. Designed like a real cyberattack, these exercises help the organization identify weaknesses, test response plans and enhance staff awareness of cybersecurity. Cyber Security Exercises provide decision-makers and technical teams with ideas for tools, techniques and procedures that can be developed to strengthen the organization's infrastructure.

Activities conducted under realistic cyber exercise scenarios improve the decision-making processes of the organization's relevant cyber defense teams, affected departments and stakeholders under stress. During and after the exercise, communication between the organization's cybersecurity team and other departments impacted by the scenario is also strengthened.

Service Components

Table-Top Exercises

Table-Top exercises involve defining the actions teams must take during a potential cyberattack. Our teams convene with the organization's cybersecurity experts to discuss how they would detect the attack, how they would respond and how systems would be restored afterward. Table-Top exercises aim to plan response processes for complex attacks without needing to simulate an attack in a live environment.

Red Team (Full Live) Exercises

A Red Team exercise is a type of cybersecurity drill that simulates a cyberattack as realistically as possible. Using the same techniques and tactics as real attackers, the Red Team attempts to access live systems and data. This exercise helps the organization's cybersecurity teams learn how they would react to an actual attack. The Red Team shares the main objectives of its malicious activities with the organization but does not reveal the details to the Blue Team. Throughout the exercise, as the organization's defenses counter each attack, the Red Team continues developing new attack vectors and advances until reaching its final objectives.

Hybrid (Combined) Exercises

In Hybrid exercises, the technical details of the scenario and the tactics of the attacking team are communicated to the organization beforehand. The attacking team refrains from using any techniques outside those outlined in the scenario. By adhering to the agreed phases, the exercise proceeds in a coordinated manner between the organization's cybersecurity team and the attacking team. These exercises strike a balance between the controlled environment of Table-Top exercises and the realism of Full Live drills. Cyber exercise scenarios must be carefully crafted according to the organization's inventory and personnel competencies. Failure to tailor scenarios to the organization's needs may result in an inability to accurately identify existing risks and predict the outcomes of potential future threats.

Scenario Design

Scenario design is the most critical phase of a cyber exercise and is vital for the exercise's effectiveness. Scenarios are created in line with the organization's security requirements and the threat environment. They incorporate realistic cyberattack types, threat vectors and attacker behaviors that the organization might face.

To evaluate how teams will respond under crisis conditions, the scenario outlines the targeted systems, attack methods to be used and response procedures. It also ensures compatibility with the organization's existing security infrastructure, taking into account staff skill levels and maturity of the infrastructure.

Scenario Execution

Scenario execution is the stage when the designed scenario is deployed in practice. During this phase, teams act according to the scenario, experiencing the processes of detection, monitoring, response and remediation. By working in coordination, teams have the opportunity to develop decision-making skills and sharpen their crisis response capabilities. Observing the steps teams follow during execution shows how the organization would manage operational processes in a real crisis. Successful execution hinges on teams taking timely action, collaborating effectively and containing identified vulnerabilities.

Analysis and Evaluation

The analysis and evaluation phase involves a detailed review of data collected during the exercise and an assessment of the exercise's effectiveness. Challenges encountered by security teams during response, the success of actions taken and any shortcomings are analyzed. Data recorded during the exercise provides insight into teams' competency levels and the resilience of the security infrastructure. The evaluation identifies vulnerabilities discovered during the scenario and pinpoints areas requiring improvement.

FAQ

What is the Cyber Exercise Service and why is it important?

Cyber Exercise Service consists of hands-on training and simulations designed to raise organizations' readiness levels against cyber threats and allow participants to experience how to act during a crisis. Exercises teach all involved—security teams, senior management and other staff—how to respond to cyber incidents. In today's environment, where cyber threats are rising, these exercises are critical for ensuring business continuity and minimizing potential damage. During exercises, teams develop response capabilities and strengthen coordination.

What types of exercises are included in the Cyber Exercise Service?

Cyber Exercise Service includes various types: Table-Top Exercises, Full Live Exercises and Hybrid (Combined) Exercises. In Table-Top exercises, attack scenarios are discussed in a non-live environment, allowing teams to debate theoretical response processes. Full Live exercises simulate a realistic cyberattack to observe how security teams operate under crisis conditions. Hybrid exercises merge elements of Table-Top and Full Live exercises to create a controlled but realistic environment. Each exercise type is chosen based on the organization's needs and staff experience levels.

Which scenarios are used during cyber exercises?

Cyber exercise scenarios are carefully crafted based on the potential cyber threats an organization may face. Exercises may include privilege escalation, data leakage, authentication breaches, ransomware attacks, phishing and more. Realistic scenarios are crucial so that teams learn how to respond and what steps to take. Internal threat scenarios—representing risks originating within the organization—can also be incorporated.

Why should exercises be conducted regularly?

The constantly evolving nature of cyber threats requires organizations to regularly test their security protocols. Regular exercises keep organizations prepared for current threats. Each exercise is structured with different scenarios and threat types to ensure that security teams remain ready for diverse challenges. Exercises allow for swift identification and remediation of vulnerabilities. By gaining experience through repeated exercises, security teams can respond more effectively and rapidly in real crises.

Which departments should participate in cyber exercises?

Cyber exercises require participation not only from security teams but also from senior management, IT, legal and communications departments. Senior management experiences the organizational impact of decisions made during exercises and learns what actions to take during a crisis. The IT department gains hands-on experience managing technical infrastructure and implementing security protocols. Legal and communications teams prepare for legal requirements and public response during a crisis. Involving all these departments ensures the organization can cooperate and adapt collectively during a crisis.

How often should cyber exercises be conducted?

The frequency of cyber exercises depends on threat complexity and organizational needs, but conducting them several times a year is generally recommended. Organizations in high-risk or critical sectors should run exercises more frequently to maintain readiness. Regular exercises keep teams prepared and test the effectiveness of security policies. The frequency may vary based on organization size, industry and security requirements. Some organizations prefer quarterly comprehensive exercises to continuously evaluate their security posture.

How does Cyber Exercise Service improve employees' security awareness?

Exercises teach employees practically how to respond to cyber threats. By experiencing different scenarios, employees become more conscious of potential threats and learn how to act accordingly. Exposure to social engineering and phishing scenarios improves awareness and compliance with information security policies. During exercises, employees learn their specific responsibilities and how to operate during a crisis.

Does the Cyber Exercise Service comply with the Digital Transformation Office's BIG (Information and Communication Security) Guide requirements?

Yes. Cyber Exercise Service is designed to meet the cyber exercise requirements outlined in the Turkish Republic Digital Transformation Office's BIG Guide. The BIG Guide recommends public institutions regularly conduct cyber exercises to elevate their information security levels. Our service offers various exercise types (Table-Top, Full Live and Hybrid) in line with these principles. The exercise process includes participation from the organization's security teams as well as managers and other relevant personnel, as stipulated by the guide. As required, analysis and evaluation follow each exercise, reporting vulnerabilities and improvement needs. Additionally, scenarios are tailored to the organization's needs and threat profile in accordance with the BIG Guide. By providing Cyber Exercise Service, organizations can demonstrate compliance with the BIG Guide and take significant steps toward strengthening public security and information integrity.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "**Privacy For You**" we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY