Benefits

Assurance
Have confidence that your current cyber security investments are delivering value.

Education
Provides an engaging, focused environment for improving understanding of cyber security at executive and managerial levels.

Demonstrate compliance
Quick, clear, non-intrusive evidence of a mature cyber security programme.

How do you know you are ready for a cyber security incident? Have you tested your cyber security incident response across the entire organisation?

We let you explore the most challenging cyber security incidents in a controlled environment. This allows you to understand what aspects of your programme are effective and what areas need further development. Exercising is a key part of delivering a security programme that meets the NIS Directive.

Why us?
Cyber security is a developing discipline and there is a lack of individuals with experience of how actual attacks are conducted. Clear Cut Cyber has world class knowledge of attacking critical networks. We understand how nation state cyber operations take place. We have used this knowledge to test and exercise at the highest level of UK Government cyber exercises.

It is important that exercises are run rigorously by independent assessors. We bring detailed military planning and rigour to delivering cyber exercises so that your security policies and processes can be assessed in an organised and objective way. Exercising scenarios must be realistic and relevant to the organisations and teams they test. Our experience of attacking critical networks allows us to create realistic scenarios for Operators of Essential Services (OES) under the NIS Directive.

Service Overview
Cyber incident management exercises test all aspects of your cyber security. They provide a holistic assessment of your cyber security and test your decision making at the technical, procedural and operational levels. During each exercise our highly experienced consultants facilitate a table top scenario tailored to your organisation. They analyse your responses and report key findings back to you.

What you get

After action report (pdf) containing:

- Full details of the scenarios as conducted
- Participants' responses
- Analysis of how effective actions were
- Analysis of how existing policies and processes performed

Executive presentation (ppt) containing:

- Concise summary of the exercise scenarios
- Lessons identified
- Recommendations

Timeline

- Consultation (2 days onsite)
- Exercise planning (3 days offsite)
- Exercise play (2 days onsite)
- Final report (1 week offsite)

Our Approach

We begin by gathering information about your key business operations and their supporting IT. This is analysed and used to generate an attack plan that tests various aspects of your cyber security processes. A strong narrative is used as a golden thread to maintain interest and context.

During the exercise we facilitate and observe. This ensures that key objectives are met and that learning and discussion points are accurately recorded. We conduct exercises in a collaborative and open manner. We have found that significant value is gained from the discussions that spontaneously occur during an exercise.

After the exercise we conduct an analysis and reporting phase. This will include an objective assessment of how existing policies and processes were applied. We also assess how effective these policies are in a challenging, realistic scenario. The final report will include lessons identified and recommendations for future improvement.

Participants

Exercise participants will be discussed during the consultation and scoping phase and should be in line with existing incident management policies. This may include:

- People responsible for business functions
- People who understand how the business functions
- People who understand how technology enables the business
- Legal and PR

What is the NIS Directive

The Network and Information Systems (NIS) Directive came into UK law on 10 May 2018 and applies to Critical National Infrastructure (CNI). The Directive applies to the energy, transportation, healthcare and digital services sectors. Each sector has a nominated Competent Authority (CA) to oversee the Operators of Essential Services (OES). The National Cyber Security Centre (NCSC) has been appointed as the technical authority for the Directive. The NCSC has written a number of guidance documents on how to comply with the Directive and has identified exercising as a key activity.

For more information please email **info@clearcutcyber.com**

CLEAR CUT CYBER

Clear Cut Cyber Ltd
71-75 Shelton Street, Covent Garden, London, England, WC2H 9JQ
Company number: 11621065. VAT Number: 315 6191 15.
www.clearcutcyber.com