Cabinet Office

epc Advise Educate Exercise Implement

# Case Study: A Major Regulated Utility Company

## Development and delivery of a command post simulated crisis management exercise to assess cyber resilience from 'server room to board room'

## Executive Summary:

### Background:

Provide an independent assessment of the company's holistic resilience capability in relation to the management of a cyber attack; from the immediate response to the management of the wider consequence. The assessment encompassed all involved, from server room to boardroom and including the CEO-led Strategic Management and Incident Leadership Team.

### EPC's Solution:
Developing Adaptive Capacity

A two-phased approach to effectively enable a baseline assessment of the company's organisational resilience:

Phase 1: Evaluate the capability of the company's cyber technical and management support team.

Phase 2: Using learning outcomes from Phase1, evaluate essential elements of the company's resilience capability including situational awareness, incident management, crisis management, crisis communications, business continuity and reputational impact.

### Result:
Validate and Review

- Make a base line assessment of the company's resilience in terms of their cyber and associated crisis management capability.
- The outcomes from the exercise informed the company's governance and proposed improvements to their existing processes, thus enabling them to improve their overall resilience.

> *We would like to express our wholehearted appreciation for the design and delivery of the exercise which stopped us thinking we were on top of the game, when we've clearly been woken up!*
>
> ***Chief Executive Officer***

> *Very well delivered exercises with informative and professional staff; scenarios were very easy to relate to the real world.*
>
> ***Chief Information Officer***

serco

## The Background:

A Critical National Infrastructure (CNI) public utility energy provider approached EPC to provide an independent assessment of their extant Business Continuity Management processes including their 'Incident Escalation and Management Procedures' to a cyber-related threat.

The aim was to assess the company's overall ability to manage cyber-attacks from the technical team/ server room; (including outsourced providers of services), through to the consequence management (business continuity and crisis communications) up to and including the CEO-led Strategic Management and Incident LeadershipTeams (boardroom).

## The Solution:

EPC recommended a two-phase approach starting with a base-line assessment of the company's holistic resilience capability within emergency management context. This involved the use of cybX services to conduct an operating model assessment from a cyber-attacker's perspective and to then develop a series of attacks as part of an overarching crisis management exercise scenario.

The first phase exercise took place in the cybX suite based at the EPC facility in Yorkshire. During which the Blue (technical) team were subjected to a series of cyber-attack scenarios, with both simulated technical and 'real world' play.

All Blue Team actions were recorded, down to the individual key stroke, time of decision and communications made to the wider UKPN organisation and other stakeholders; (referred to as the White Team and led by the Chief Information Officer (CIO) who provided the necessary business-led decision-making during the cyber-attacks.

Phase 2 of the exercise was conducted within the company's London HQ. During Phase 2, and using learning outcomes from Phase 1, the company's executive (CEO led ) and senior management teams were exposed to the consequence and impact of the initial cyber-attack. During Phase 2, essential elements of the company's resilience capability was evaluated including; situational awareness, incident management, crisis management, crisis communications, business continuity and reputational impact.

## The Result:

Using empirical data resulting from the exercise activity, EPC were able to make a baseline assessment of the company's resilience in terms of their cyber and crisis management capability. The immersive and experiential learning environment created by EPC helped to increase mutual trust, shared understanding, communications and collaboration between the various participants involved.

Further, the exercise provided a number of lessons. Some of these are:

- Adjusting the commercial service provision from third party cyber security service providers, so that the company has better visibility and control.
- Identifying gaps in incident response procedures and skills in a cyber-attack environment, despite having an advanced crisis management and business continuity/disaster recovery capability.
- A recognition that the dynamic, complex and uncertain environment cyber-attacks can create requires clear governance to be in place and prior consideration of the consequences created by different actions during the response. This includes being better able to engage in dialogue pre-breach with external stakeholders, including regulators.

Following discussion with the CEO and board, the EPC was invited to conduct a more in-depth analysis of other selected elements of the company's resilience measures.

### About Us

EPC is the UK's leading centre for organisational resilience, delivering emergency and crisis management, business continuity, cyber resilience, event and public safety training, exercising and consultancy services. Our highly experienced, industry leading experts work closely with organisations of all sizes to deliver our services to both public and private sectors in the UK and across the world.

For more information please visit:
www.epcollege.com or email:
enquiries@emergencyplanningcollege.com