Multi-billion-dollar megaproject

CASE STUDY OVERVIEW

A series of crisis simulations successfully tested and improved cyber response plans for a multi-billion-dollar project in its infancy. Building cyber resilience into company foundations at an early stage, to reduce serious business and reputational risk.

OUR MISSION

Berwicks received an invitation to tender from a large company managing a high value megaproject. This relatively new business was seeking proposals for a series of cyber crisis simulation activities. And with consultants on our team who are highly experienced in cyber response and simulations, we were well placed to apply.

The brief was to run a series of three simulations. They were to be based on realistic scenarios that could challenge the functioning of the company and even pose an existential threat. Exercises could involve a number of different cyber issues:

- **Malware or ransomware attacks.**
- **Malicious insider activity.**
- **A power failure impacting the whole site.**

The focus of these simulations was operational and communications response, rather than technical incident response. Strategic communications was an integral part of the brief.

Competing against significant competition, Berwicks was successful and awarded the contract.

MISSION ACCOMPLISHED

- **Three cyber crisis simulations involved key leaders and stakeholders.**
- **Senior executives tested under pressure.**
- **Cyber-attack response plans effectively tested and improved.**
- **Important alerting and information management systems enhanced.**

> **“For this project, we delivered much more than cyber crisis simulations. We established long-term cyber resilience from the outset, using an approach that’s not like other consultancies. The potential cyber risks were significant, for the reputation and operations of the company. We stepped in to ensure their cyber security is fit for purpose – now and into the future.”**

Richard Youngs, Managing Director, Berwicks

Multi-billion-dollar megaproject

HOW WE DELIVERED

We immediately started working with the client's Computer and Information Services (CIS) team to:

- **Review** the existing cyber incident response plan.
- **Plan and design** three scenario simulations to rigorously test it.

A team of highly experienced Berwicks consultants travelled to the client's location to run the simulations.

The commitment of a whole organisation is fundamental to achieving robust cyber resilience. So, we went beyond the CIS team and involved senior executives in the simulations, as well as the departments they lead.

The simulations were stage managed by the Berwicks team, who gave participants scenario updates throughout the exercise that they had to respond to. Each simulation was followed by an immediate debrief to collect feedback and discuss opportunities for improvement. A detailed report was then prepared, to guide internal planning and decision making around cyber crisis response.

OUTCOMES

During the simulations, senior executives were put under pressure and shown how they need to perform in the event of a cyber-attack. Hundreds of people from across the business were also involved, so everyone now understands their role should a real cyber-attack take place.

Existing cyber response plans were rigorously tested and improved where necessary. Alerting and information management systems procured specifically for communications in a cyber-attack were tested and improvements identified.

Before the simulations, the client had a broad understanding that cyber-attacks posed a significant enterprise-wide risk. After the simulations, they were delighted that relevant cyber risks had been spotlighted so effectively.

WHAT NEXT?

Our client realised that cyber is just one potential route into a crisis for the company. A new resilience workstream has been established to reduce and manage broader risks across the whole enterprise.