Case study – Hong Kong

Cyber threat understanding

A global oil and gas company believed that they could be targeted by a variety of cyber threat actors. The company asked Control Risks and MWR to conduct a holistic and comprehensive assessment of the threat that they faced and a compromise assessment to understand if there was any evidence of breaches on the Client’s systems already.

Control Risks and MWR developed a tailored threat assessment that detailed the specific cyber espionage, crime and activist threat that faced the client, with supporting case studies. The threat assessment explained the likely assets that would be targeted, the intent and capabilities of different threat actors and the typical approach that would be taken by an attacker. It was discovered that the nature of the threat faced by the client was to a large part determined by a few critical elements of their corporate strategy.

In parallel with the threat assessment, Control Risks and MWR conducted a compromise assessment to understand if there was any evidence of breaches on the Client’s systems already. Through working with certain members of the Client’s IT team, Control Risks and MWR were able to uncover a number of anomalies. These anomalies, when contextualised with other data and the threat assessment provided the Client with an evidence base of the specific threat that they were facing.

By understanding the level and nature of the cyber threat and with an evidence base to support this, the client was able to begin scoping an appropriate cyber defence strategy that protected the highest value assets from the specific cyber threat that they faced.