Contractual Security Due Diligence

Overview

Almost every business irrespective of size relies on third parties to deliver support services.

A study conducted in 2019 by YouGov highlighted that prior to the COVID pandemic seven in ten British businesses outsource to third parties, this means that 70% of B2B decision-makers saying they've handed off key services to third parties. Only a quarter (25%) say they've never done so in any area of their organisation and this number is only likely to grow further.

Working with partners and suppliers increases the opportunity for access to skills, technology, scaling and wider economic growth. But it can pose a challenge in managing Information Security risk across many organisations.

A breach of your customer data from a third-party supplier is equally as damaging than if it were taken from within your own environment, so organisations must maintain the cyber readiness of partners and suppliers. A one-size fits all approach will seldom address the complex needs of a service involving many third parties.

A common mistake made by some risk management strategies are that they focus on a point in time (usually at the beginning of the contract) and never continue as the contract matures, yet the ever-evolving landscape pertaining to cyber threats means that it can be difficult to ensure that suppliers and partners are continually maintaining their cyber posture in accordance with your own organisations risk appetite and tolerance levels.

It is essential (and indeed good practice) that you identify potential third-party cyber risks early on and not only ensure alignment with your organisations risk appetite but also set up an appropriate governance structure which sets out and conducts regular assessments, the findings should be regularly reviewed and reported on as part of the management information (MI) regime

Capita is the primary contractor for many of the UKs long-running major programmes involving large consortia of partners and technology providers. We are trusted to ensure that sensitive data is kept secure across these complex networks and systems. We bring this wealth of experience to our **Contractual Due Diligence** service and are ideally placed to advise on the best practices and approaches to ensure your third-party network has a resilient approach to Cyber including the most appropriate security controls.

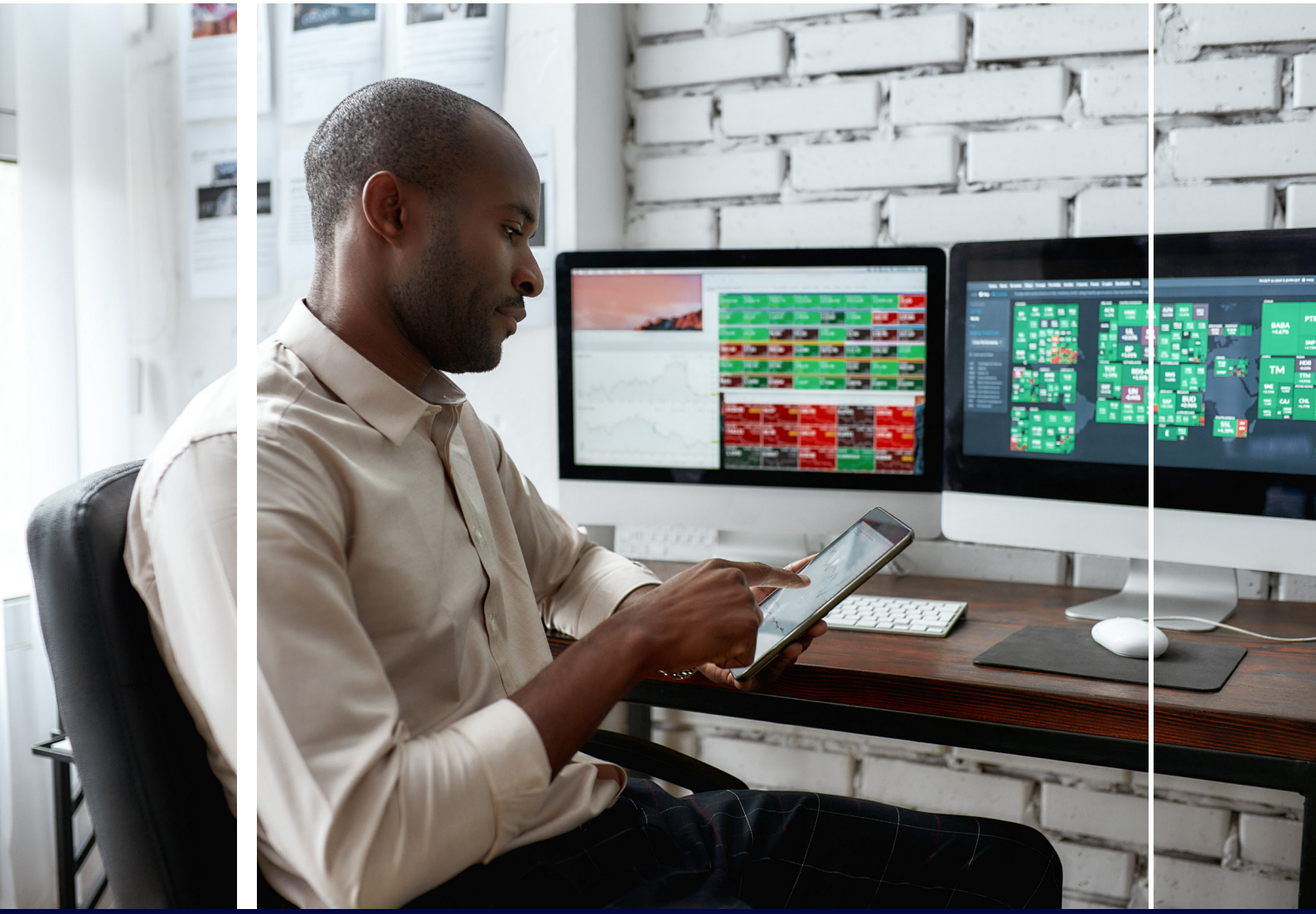
Capita

Our approach

- Define Risk Tolerance in line with the client risk appetite, agreeing alert thresholds and communication processes for incidents.
- Map current vendors
- Understand vendor criticality and how they link into critical business processes(CBPs)
- Measure vendors by assessing them using Audit and Maturity assessments
- Set up and agree regular monitoring and review points throughout the duration of the partnership including (but not exclusive to) data classification, data storage, handling and data destruction methods post partnership

Markets / Industries

- All



For more information please contact:

Jim Fox CISM, MBCS, MSyI
James.fox2@capita.com