BREACH READINESS ASSESSMENT

A focussed audit aimed at answering one critical question –
'Is my organisation data-breach ready?'

SECURITY BREACH

HACKING

INTRUS

23%

74%

56%

18%

This assessment scores the Breach Readiness capability of a specific group of people and how they respond to a specific cyber-attack scenario against a distinct critical asset.

This audit is performed in conjunction with and during our Cyber Crisis Tabletop Exercise (CCTE) and it measures and scores various attributes of the exercise and the participants during the tabletop exercise.

Benefits:

- Demonstrates how prepared a select group of staff are to respond to a specific cyber-attack on a critical asset or assets.

- Allows you to track year-on-year progress of your readiness to demonstrate tangible progress and improvements.

- Satisfies current and future regulations that demand organisations carry out structured cyber tabletop exercises.

- Allows you to test your plans, procedures and staff in a safe but near-realistic simulated environment without disrupting regular business operations.

What We Examine:

As part of our Breach Readiness audit, we will:

- Carefully examine incident response policies, processes and procedures.

- Understand the key participants, their role and context.

- Review past incidents, outages and cyber-attacks.

- Understand your critical assets and processes.

- Evaluate recent security assessments.

Stakeholders:

This audit requires us to create a fairly detailed cyber-attack scenario and hence we will need to speak to one or more resources who can support us in creating a compelling scenario.

Sample "Spider Chart" measuring your Breach-Readiness
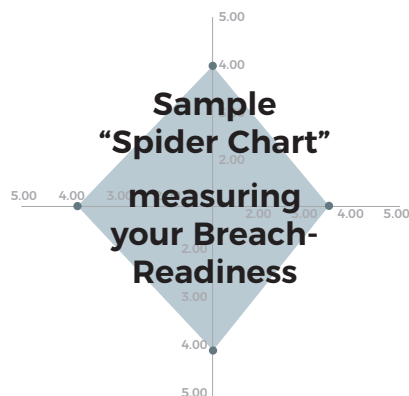
Formal Score and Tangible Improvements.

Our Cyber Crisis Tabletop Exercise (CCTE) helps answer one of the most important questions for the CEO and the executive management – "Is your organisation breach ready?"

Sample "Spider Chart" measuring more than 10 attributes

Put another way, it seeks to examine if your organisation is capable of rapidly detecting, effectively responding to and resuming or carrying on its business operations uninterrupted after a cyber incident.
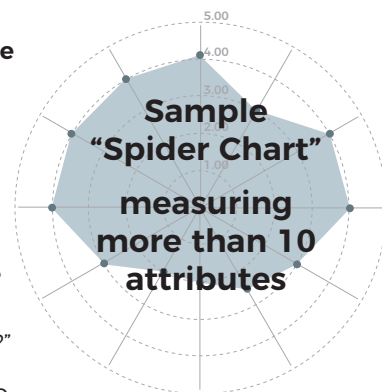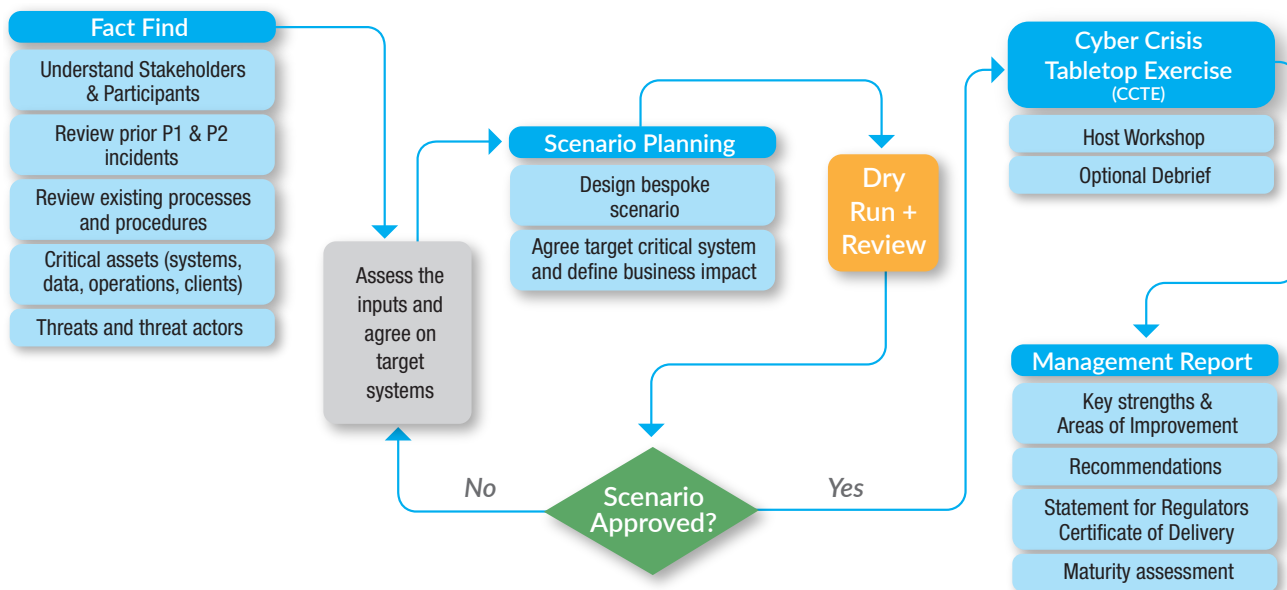
Our approach:

The image below describes our detailed approach to conducting a Breach Readiness assessment. Similar to our other audits, the process is fairly straightforward. We listen to and obtain information about your organisation, its critical assets, response plans and the role of key stakeholders during and after an attack.

We, then, create a detailed attack scenario storyboard and a corresponding presentation which will be used during the Cyber Crisis Tabletop Exercise (CCTE) workshop.

Throughout the exercise, we will either record or closely monitor the participants and assess several attributes to arrive at a Breach Readiness maturity score. .

Fact Find
- Understand Stakeholders & Participants
- Review prior P1 & P2 incidents
- Review existing processes and procedures
- Critical assets (systems, data, operations, clients)
- Threats and threat actors

Assess the inputs and agree on target systems

Scenario Planning
- Design bespoke scenario
- Agree target critical system and define business impact

Dry Run + Review

Cyber Crisis Tabletop Exercise (CCTE)
- Host Workshop
- Optional Debrief

Scenario Approved?
No / Yes

Management Report
- Key strengths & Areas of Improvement
- Recommendations
- Statement for Regulators Certificate of Delivery
- Maturity assessment

Output:

We will provide you with a formal audit report with a maturity score for your Breach Readiness along with a breakdown of the additional observations made during the tabletop exercise. The report also provides easy-to-understand recommendations on improving the score and closing the gaps.

More information on this specific assessment is available in our CCTE page and brochure.

Note: *The Breach Readiness audit does not conduct a comprehensive audit of your IT and/or cybersecurity controls. We do a cursory review of your existing processes, procedures and incident response related documentation.*