Interview Protocol/Guide: Cyber Risk Assessment Current Practice

1 Preface

The following question set and notes are to be applied during the preface phase.

- Reiterate the purpose of the interview based on the interview guide, and the expected timescale
- Confirm the participant knows the full interview will be recorded, and that they will be told when the recording is due to begin, and when it is due to end
- Turn ON the recording now
- What do you understand cyber security risk assessment to include?
  Definition: Risk assessment identifies, assesses, and articulates risks to an organisation. Risk assessment informs risk management decision making, and it requires technical, security, and business skills and knowledge.

2 Risk Assessment

The following question set and notes are to be applied during the risk assessment question phase.

- What data are you required to collect for use within your existing risk assessment methodology?
  Note: Read back the data collected and ask the participant to confirm
  Probe: If any collected data relates to attacker, cost, difficulty, time, or risk to attack - ask for elaboration on how that data is collected and where from
- Once you have acquired the relevant data, how is it applied within your existing methodology to derive cyber risk?
  Probe: Focus on any relevant data mentioned above

3 Risk Communication

The following question set and notes are to be applied during the risk communication question phase.

- How is the output of this methodology used to communicate cyber risk?
  Note: If unclear, prompt with examples such as RAG, percentage, graphical, etc.
  Probe: Where adversarial cost or attackers are included, explore further
- With whom do you usually convey the risk assessment results?
  Probe: If unclear mention this may be management or technical/IT staff etc.
- Do there exist any challenges in the conveyance of cyber risk through the use of your existing methodology?
  Probe: Refer back to who they convey this risk to, ask if this contributes to challenges, or if recipient is technical, whether they have to simplify for management

4 Adversary Importance

The following question set and notes are to be applied during the adversary importance question phase.

- How important is it in your risk assessment to consider the adversary and their capability?
  Note: Assets, resources, level of technical capability, or tenacity
  Probe: If positive response - What specifically do you discover or know about potential adversaries which pose a threat to your clients?
- Do you believe conveyance of cyber risk through "cost" could provide a more effective narrative? More specifically, the cost to an attacker seeking to compromise a client's system.
  Note: If clarification is needed, explain cost model understood so far with time, financial, and accepted risk cost
  Probe: Why effective/not effective?

5 Conclude

The following question set and associated notes are to be applied during the interview's conclusion.

- What do you think of the effectiveness of current risk assessment methodologies?
  Probe: Why effective/not effective?
- Confirm the interview questions have been completed and ask the interviewee if they would like to add anything in addition which may be relevant
- If supporting documentation has been described and offered throughout, politely remind interviewee to send via email
- Turn OFF the recording now
- Thank interviewee for their time
- Inform interviewee that if at any time they think of any points deemed relevant to the discussed topic area, that I would greatly appreciate them being sent via email
- Reiterate the options for withdrawal as described in the participant information sheet