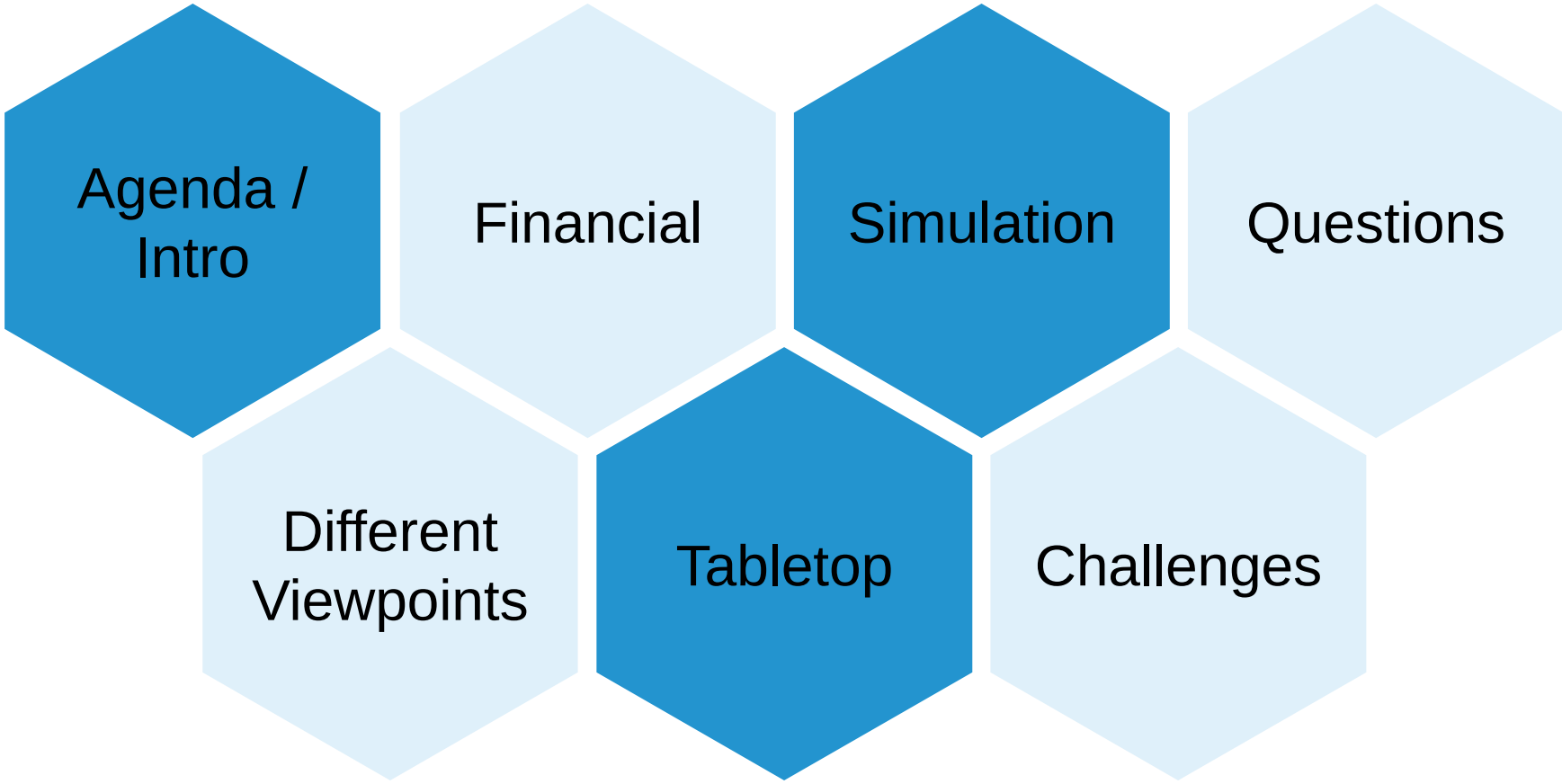
War Games, Simulations, and Scenarios: Preparing Organisations for Long Term Cyber Resilience

Justin Clarke-Salt

The Future of Cyber Risk Conference
24th July 2019

Agenda for today



Different Viewpoints

- What question are you looking to answer?
  - If X happened, how much could it cost?
  - If X happened, could we effectively respond?
  - If X hacked us, could we detect it and respond effectively?

- Scenario design and exercise impartiality are important
  - Make it hard – it may well pay off
  - Debrief thoroughly

- Examples we'll talk about
  - Financial modelling
  - IR Tabletop
  - Red Team testing (CBEST etc)

Financial

“So, how much could this cost???”

Why are we talking about Financial models? Isn't this a cyber conference?

- Scenario development:
  1. Technology asset (mission critical technology)
  2. Cyber event happens (technology compromised)
  3. Threat actors/triggers (how does the threat cause the event?)
  4. Areas of impact (what are the commercial ramifications?)
  5. What are the risk mitigation strategies given the described scenarios?

- Keeping the physical and non-physical in mind

Commercial Impacts

How can we analyse our economic exposure from the risk scenarios identified?

What are the commercial impacts of each scenario modelled?

Case Study: Wind Farm Operator

“About €200 million”

Tabletop

“If that happened to us, would we be able to respond?”

Why Tabletop?

- After everything has gone wrong is not the time to be learning what to do in an emergency
  - Make sure you debrief and learn though
- People / Process / Technology
- Key stakeholders and key decisions
- Cyber risk is evolving – are your plans?

Case Study: Mid-sized Organisation

“We should figure out who should make that decision”

Simulation

“Could we be hacked like them?”

Simulate what?

- Test / Simulation / whatever
- Common elsewhere – not necessarily in Cyber
- Two common/popular approaches
  - Red Team
    - CBEST, iCAST, TIBER, GBEST, TBEST, SpaceBEST
  - Breach Simulation
- Purple Team

Case Study: CBEST

”APT simulation, Bank of England style”

Regulatory Red Team (Insurance Company)

Scenario 1 (Organised Crime Group)

- OCG with links to FIN7, targeting payment systems for payment redirection
- Infiltration via spear phishing, posing as a partner organisation
- Use of access to insurance policies to update bank details and redeem/refund policies to accounts under the OCG's control

Scenario 2 (Cyber Extortion Group)

- Extortion group with ransomware similar to SamSam targeting company for large ransom over critical business functions
- Infiltration via gaps in perimeter network security
- Targeting the main quotation generation system and demanding a ransom in cryptocurrency

Scenario 3 (Nation State Actor)

- Simulating a Chinese Ministry of State Security actor
- Infiltration via compromising a trusted third party – e.g. managed service provider
- Thefts of PII for large data sets of customers for organisations in potential geopolitical rival states.

Contact List

Justin Clarke-Salt
Managing Director
Aon
Cyber Security
+44 (0) 7538 823 165
justin.clarke-salt@aon.co.uk

Legal Disclaimer

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber security, risk and insurance management, investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Cyber security services provided by Stroz Friedberg Limited and its affiliates. Cyber risk services provided by Aon UK Limited and its affiliates.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

aon.com/cyber-solutions