
Ministry of Defence
Army Exco Cyber TTX
Georgie Rice
Asst. Hd Cyber Security CSOC
ARMY
BE THE BEST

Background

Background – Respond and Recover

EXCO 2022

AIM: To understand and rehearse decision making in the event of a Complex Cyber Incident

SCENARIO: Ransomware attack on Royal Military Police IT system

ECAB 2023

AIMS: Increase awareness of cyber threats and potential impacts. Allow ECAB to understand responsibilities across the Army during a crisis. Leave the event with a greater awareness of what is required by senior leadership in the event of a cyber incident and support the development of Army strategic policy and Crisis Response Operating Procedures

SCENARIO: Supply Chain attack on Boeing compromising a component part of the cooling system of the Apache helicopter. Part was common across D and E variants, leaving no resilience in attack helicopters now deemed unsafe to fly.

Background – Understand and Prepare

The Army Strategic Crisis Management plan was tried and tested during a live incident, therefore a different approach was taken for the third iteration of Senior exercising. Moving from RESPOND and RECOVER exercising to UNDERSTAND and PREPARE.

AIMS

To focus Army ExCo on their individual and collective responsibilities for the risks from cyber challenges to operational effectiveness and modernisation of the Army

- Transform the ExCo approach to cyber risk management, focussing on individual and collective accountability and responsibility for cyber risk. Including better and consistent support for the Army Cyber Governance Risk and Compliance Board.
- Ensure integration of through life cyber security in planning, delivery, and sustainment of operational activity.
- Gain an understanding of Army critical outputs and dependencies on other TLBs, Government departments, or agencies.
- Strengthen our approach to cyber security by initiating behavioural and cultural change at the highest level of the organisation.
- To consider what the Army should be doing now to ensure we are better prepared for future warfighting.

Background

PRE MORTEM DESIGN

- Looking forward to examine a future catastrophic event and working backwards to determine what can be done now to plan and prevent that happening to the best of our abilities.
- Developed in line with the Defence Wargaming Handbook and the Red Teaming handbook.

SCENARIO

- A failure of FLF deployment in 2027 for a NATO exercise due to a coordinated cyber campaign.
- Looking through the lens of ‘our soldiers’ ‘our capability’ and ‘our authority.’
- Each vignette was viewed both from the adversary / enemy perspective and the military perspective.

What could be improved

What could be improved

- Time allocation

- Understanding of decision making at each level
  - Are we exercising the right people in the right way?

What went well

What went well

- Introspective self-realisation - participants derived the key insights themselves

- Cyber Security beginning to be recognised as a collective responsibility
  - Training Audits
  - Quarterly Risk Reporting
  - Education and awareness programme

Close