Exercise Tri-Unity to improve cyber awareness

A bespoke cyber exercise product delivered to North East forces involving numerous and broad key stakeholder departments to improve cyber awareness and promote understanding of risks and impacts and put business continuity plans in place.

First published
20 February 2025

Key details

Does it work?	Untested – new or innovative
Focus	Prevention
Topic	Community engagement Crime prevention Cybercrime including fraud Digital
HMICFRS report	**PEEL 2021/22: An inspection of the north-east regional response to serious and organised crime**
Contact	Paul Maddison
Email address	nerccuprotect@durham.police.uk
Region	North East
Partners	Police Health services Local authority

Key details

Stage of practice	The practice is implemented.
Start date	January 2024
Completion date	June 2024
Scale of initiative	Regional
Target group	Communities

Aim

Exercise Tri-Unity – was designed from the ground up and includes real world learning from cyber-attack victims in the North East. It is aimed at key decision makers within the force, to include the following participants.

- Gold
- Silver
- Intelligence
- Custody
- Response
- IT
- Information management
- Force operations/incident manager
- Media
- Any other functions as deemed necessary

This exercise is a standalone exercise intended to explore, test and improve internal cyber capabilities of the North East forces around response, recovery, investigation and education to

cyber threat.

Intended outcome

The objectives of the exercise are the improvement of an in force participant's capability to:

- explore and address cyber-security challenges
- understand the impacts of an attack across different departments within the organisation
- implement appropriate recovery procedures
- facilitate an understanding of the dependencies and interdependencies of information technology, risk management and business continuity
- test the implementation and understanding of command and control within a cyber incident
- test the reporting and IT escalation processes
- test liaison with the force specialist Cyber-crime Unit & North East Regional Specialist Operations Unit
- capture any technical interdependencies between internal and external systems identified through the course of the exercise
- capture learning outcomes for continual development of incident response process
- identify gaps in demonstrated capabilities or current plans, policies, and procedures
- understand the implications of losing trust in IT systems and capture the workarounds for such losses
- expose and correct weaknesses in cyber security systems or physical infrastructure

Description

The exercise was designed from the ground up and includes real world learning from cyber-attack victims in the North East. It is aimed at key decision makers within the force.

The exercise is facilitated by protect officers from the North East regional special operations unit cyber crime team. The facilitators will not provide right or wrong answers to scenarios but will provide guidance on best practice around incident response. Forces decide what is right according to their own incident response and business continuity plans.

Participants are split into teams, consisting of players from the same department. Each team is assigned a table to discuss among themselves until the facilitator open the discussion to the wider

group. A “scribe” is assigned for each team from the contingency planning section whose role is to document any learning or gaps from their assigned table to feed a debrief.

The delivery is via an interactive slide deck (PowerPoint) consisting of audio, video, and static inputs accessible to all group participants. Papers are presented to a specific member of the team of tables whose role it is to decide what to do with the information.

Evaluation

The initiative will be evaluated in 2025 after the next round of training.

Overall impact

The exercises have allowed Forces to review, develop, and improve their own business continuity plans. Discussion and forward planning are just a few of the positives to come from Tri-Unity. It has shown all departments that cyber is not just ‘an IT issue’ and should be at the heart of the business continuity planning for all departments.

The roll out of service is now offered to other blue light service providers and areas of local government.

Feedback from exercise participants:

- ‘The managers and I in the team will now produce a department action plan to make sure we have contact details and key documentation in a physical file or secured location’
- ‘It was a good eye opening, and sitting with the appropriate departments was useful. I gained an understanding of what other departments do and how they would respond.’
- ‘In my role as BC manager I will reinforce to departmental plan owners that they need to be specific and realistic about what they include as contingencies in the event of loss of ICT by whatever cause.’
- ‘Digital Services now understand they require a better understanding of other departments and their responses.’
- ‘Good scenario information. Good to see how realistic AI is today and the further possibilities moving forward.’
- ‘Multiple parts of the organisation represented, each with varying degrees of experience when it comes to business continuity.’

Learning

- All departments within the police service are encouraged to complete this training.
- Some exercises were not as well attended as others as potential participants thought the training did not apply to them. The senior leadership team (SLT) attended training and saw first-hand how essential it was to ensure business continuity. Their feedback will reach those who did not attend which will help boost attendance for the 2025 sessions.

Copyright

The copyright in this shared practice example is not owned or managed by the College of Policing and is therefore not available for re-use under the terms of the Non-Commercial College Licence. You will need to seek permission from the copyright owner to reproduce their works.

Legal disclaimer

Disclaimer: The views, information or opinions expressed in this shared practice example are the author's own and do not necessarily reflect the official policy or views of the College of Policing or the organisations involved.

Tags

Cybercrime