Appendix A – Ex Troy scenario overview

- Exercise Troy simulates a major cyber incident to test KCC's resilience and preparedness. The scenario begins with a targeted phishing email sent to hundreds of staff, designed to appear as a legitimate communication about annual leave. This email contained a malicious link, which, when clicked by several employees, triggers a ransomware attack that disrupts access to critical council systems.
- As the incident unfolds, the council face escalating challenges. Key services (including social care, payroll, HR, and customer-facing portals) become inaccessible due to data encryption. The public quickly notice service disruptions, leading to an increase in contact centre activity and media interest. ICT teams respond by investigating the breach, issuing communications to staff, and implementing precautionary system shutdowns to contain the threat.
- The exercise progresses to a stage where systems remain offline for an extended period, with partial restoration only possible through offline backups. A ransom demand is made public, increasing scrutiny from both the media and affected residents.
- The exercise concludes with systems only partially restored, prompting the council to implement a phased recovery plan. Proactive measures are taken to address and correct misinformation spreading on social media.