**Service Definition**
**Cyber Incident Response Simulation**
**Introduction**
Cyber threats targeting the UK public sector are increasing in frequency, sophistication, and impact. As critical services and citizen data become more digitally dependent, organisations must be able to respond swiftly and effectively to a range of cyber incidents.

A well-designed Cyber Security Incident Response Simulation (CSIRS) provides a safe, controlled environment to test current capabilities, improve coordination across teams, and build confidence in the Local Authority's ability to manage a real-world cyber crisis.

This simulation also supports compliance with relevant standards such as the NCSC Cyber Assessment Framework and evolving regulatory expectations under UK GDPR and NIS2.

**The Objective**
To strengthen the readiness to respond to a plausible cyber-attack by simulating a realistic incident scenario, facilitating cross-functional collaboration, and identifying gaps in current response, continuity, and reporting procedures.

**Scoping**
A scoping meeting will be held at the outset of the engagement to fully understand your organisation's aims, goals and expectations relating to information security. A detailed proposal will then be prepared outlining the stages involved, milestones and the level of both NTA and your organisation's input required to meet requirements.

**Key Outcomes**
The engagement sets out to achieve the following outcomes:
- Test of the crisis coordination and decision-making through simulation of a plausible, realistic cyber attack
- Improve the understanding of non-technical and technical crisis response roles
- Practice working as a team whilst dealing with a complex, business-critical event
- Identify gaps in resilience arrangements, continuity plans, recovery plans, legal response, and external breach reporting
- Identify key actions required to enhance the cyber resilience

**Optional Enhancements**
To further enrich the participants' experience we can involve external specialists in both the preparation and workshop phases, for example:
- Data Privacy specialists to explore UK GDPR / breach notification implications
- Legal and regulatory specialists to simulate internal and external advisory interactions
- External Cyber Security Incident Response (CSIRT) teams, if applicable, to practice the interaction during a serious security breach.

**Service Overview**
The simulation is delivered as a 1 to 2 day in-person workshop based on an interactive, scenario-based exercise tailored to the Local authority's threat profile (e.g. ransomware, data breach, or service disruption).

The scenario will be based on real-world cyber incidents affecting the UK public sector, the Local Authority's IT environment, as well as business continuity, disaster recovery and crisis

**Service Definition**
**Cyber Incident Response Simulation**
management plans. The scenario will unfold in sequential stages during the simulation, beginning with a service outage and progressing to a ransom demand and subsequently to a data breach, accompanied by various unforeseen developments (a.k.a. injects) to reflect the changeable nature of cyber security events.

We encourage multi-disciplinary participation across IT, legal, data protection, communications, and leadership teams during the planning and preparation phase, as well as in the workshop itself.

**Service Management**
You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling onsite delivery, ensuring reports are sent out in a timely manner, scheduling follow up activities and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

**Ordering and Invoicing Process**
Once the scope of work and number of units/days required has been agreed between the customer and NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

**Customer Responsibilities**
The customer is responsible for providing relevant access, contact details and documentation as required, with a commitment from key stakeholders to engage with NTA to ensure the most successful outcome from the service required.