Health & Social Care Information Centre

HSCIC Security Operations Proposal

Rob Shaw, Director of Operations and Assurance Services

14/05/2014

Purpose

1. To provide the Board with the results and considered recommendations for the implementation of a security operations function in support of the HSCIC Strategy objectives of keeping data secure and delivering the national technology services.

Actions Required

2. To endorse the recommended approach to develop the required business case within the HSCIC Cyber Security Programme which will establish the required funding streams and HR process for recruitment.

Progress to date

3. The EMT has already provided endorsement to the high level approach described within this document, at their meeting in February 2014.
4. A high level briefing has been provided to the newly created Cyber Security Leadership Forum chaired by NHS England, providing an illustration as to how the Operational Security framework can help to coordinate and deliver the capabilities required to meet the challenges of the wider Cyber Security Programme.

Background

5. The review was initiated following engagement with the SIAM programme in relation to the required functions and services to support internal delivery of national programmes and services. Early engagement has fostered a strong working relationship which has supported the delivery of the review. An independent security expert was brought in to complete the review in an un-biased manner.
6. Engagement with larger programmes and other support areas has been conducted through a series of workshops, teleconferences and email exchanges.
7. During the review, requirements in relation to the provision of services and functions for the benefit of the wider health and care system have been identified. These have arisen from engagement with DH and NHSE in relation to the provision of Cyber Security co-ordination and monitoring functions at a national level to support ministerial strategies.
8. The full report of the review recommended a Target Operating Model (TOM) which is the basis for a scalable, resilient and industry aligned operational function which will deliver the required services and expertise to support the HSCIC and the wider system. The TOM includes a revised security function structure, engagement model and target capability model which will guide the implementation and resource guidelines within the report are in addition to existing capability.
9. The report has been assessed internally by the Infrastructure Security Team (IST) and the recommendations have been aligned with current capabilities and responsibilities. The recommendations section provides final detailed recommendations, highlighting any deviation from the independent report. This report has been provided alongside this brief.

Recommendations

10. The IST has been engaged throughout the process and provided information on current capabilities and responsibilities. The recommendations endorsed by EMT were:

    a. The proposed structure is endorsed as the strategic function for security operations

    b. That a more detailed assessment of the business case, required funding and tooling, and options for migration of skilled staff into the function was undertaken. It is envisaged that this work will be completed by July 2014.

    c. The current IST to be reformed to create the Security Management function including migration of other specialist resources across the organisation which would best sit with a central function offering services back to programmes, projects or functions.

    d. The current Operational Security Team (OST) to be reformed and enhanced to provide the Incident Management function which would renamed to the Operational Incident and Assurance function. This function would include current assurance capabilities such as Information Governance Statement of Compliance assessments, Commercial Aggregator assurance and any other IG or Security assurance functions which would benefit from centralisation

    e. The Protective Monitoring function was not recommended to be resourced internally. This specialist function was considered to be best served through a strategic partnership with a dedicated provider in order to leverage best cost and functionality. Management of this function would be undertaken by the Operational Incident and Assurance team.

    f. The Security Engineering and Tools function would be a completely new function which is an established capability in organisations across other industries. It was recommended that this function is established quickly to support the development of key national services such as SPINE2, IAM2 and care.data.

    g. The overall function to be supported by a strategic partner providing additional expertise, niche skills or experience, specialist services and a flexible resource pool to cope with peaks in function demands.

    h. The funding model for the function would be split between corporate GIA, programme level capital and revenue funding, and funding for nationally focussed capabilities provide by DH.

    i. Further assessment of the intended resource structure has been undertaken recently. Initial findings suggest a significant proportion of the required resource is already in place within existing HSCIC work areas. Additional resources are required to fulfil the Target Operating Model, but can potentially be recruited to augment existing capability, as the TOM develops during the medium to longer term.