CQC response to the independent, external review of the data security breach involving the loss of DBS certificates from CQC premises in Newcastle

Following the data security breach involving the loss of DBS certificates, I commissioned an independent, external review of the incident and the subsequent internal investigation and follow up.

The report has now been received and recognises that the information security architecture within CQC is fundamentally sound. It does however note that there is a mismatch between that architecture and uniform, practical implementation of this by some staff. In relation to this point the report recommends that work is carried out to strengthen the organisation-wide information security culture to allow and enable CQC to become the exemplar organisation that we aspire to be in this area.

The report confirms the findings of the initial, internal investigation and report as well as making six recommendations. Those recommendations are being followed up now and are being incorporated into a wider programme of work to embed information security and governance into CQC culture. This work and progress on it will be overseen by the Information Governance Group (IGG) chaired by the Senior Information Risk Owner (SIRO). The report recommendations and CQC actions to respond to them are:

1. ***CQC should consider information risk to be by default an integral element of all projects which are subject to formal project management. If a decision is made by the SRO* [Senior Responsible Officer] *that the circumstances of a particular project make information risk irrelevant then that decisions should always be documented and endorsed by the SIRO.***

We will ensure that all projects are required to consider information risk and that a record of those decisions is forwarded to the CQC information security and governance teams where they can be reviewed and challenged as necessary. We will also ensure there is a requirement to check that information risk has been considered when proposals are reviewed by the Investment Committee and the Operational Development and Coordination Committee (ODC).

This action is being held by the Information Security manager to be completed by December 2016.

2. ***Existing contracts with third party suppliers should be reviewed to ensure that they provide for the provision of audit information in real time for the purpose of managing incidents or investigating wrong doing. Future contracts should include this provision by default.***

CQC uses the Crown Commercial Services framework contract wherever possible. The contract includes comprehensive security clauses and refers suppliers to compliance with our internal security and governance policy. We will review the exact content of those security clauses and determine our right to audit and test against them as well as develop spot checks with our suppliers within the contract management process. If a framework is not available then CQC uses our own contracts which cover the right to audit.

This is a joint action held by the Head of Commercial and Contracts in conjunction with the Information Security manager to be completed by December 2016.

3. ***Once the new crisis management plan has been formally approved it should be exercised (perhaps with a complex data loss incident scenario involving electronic data).***

We have agreed with CQC's business continuity management team for the schedule of testing to include this scenario as one of the first tests to be carried out this year.

This action is held by the Business Continuity manager to be completed by December 2016.

4. ***The IGG risk register (risk 25 mitigating actions) should be expanded to include the normal requirement for non-CQC visitors to CQC premises to be appropriately supervised.***

We have amended this risk and are finalising arrangements with the estates and facilities team for all visitors and contractors to be appropriately escorted whilst in CQC offices.

This action has been completed by the Information Rights manager.

5. ***The IGG risk register should have an additional risk fully addressing information security risks in the CQC supply chain.***

We have included a new risk covering contract and supply chain management on the IGG risk register.

This action has been completed by the Information Rights manager.

6. ***CQC should embark on a programme of security culture change so that they can become an exemplary information security organisation in the context of "Safe Data, Safe Care".***

This action is acknowledged within the report as being the most challenging recommendation to address.

We will engage with other organisations to identify good practice and staff engagement strategies including training, role modelling by managers and organisational spot checks. Involvement of the CQC Academy team will be a key part of addressing this action.

This action will be held jointly by the Information Security and Information Rights managers overseen by and with assistance from the IGG. It is the subject of the wider information security and governance work plan and will be scheduled for completion during 2017. However, it is planned that steps will be taken to improve the security culture incrementally towards an exemplar level.

I am asking the Audit and Corporate Governance Committee (ACGC) of the Board to assure the implementation of these recommendations, as well as our wider programme of work to ensure that CQC meets the information security and governance standards which the organisations we regulate are expected to comply with. The ACGC may also want to examine the possibility of including these recommendations as the subject of internal audits to provide assurance that our processes in this area are robust.

David Behan
Chief Executive
22 September 2016