Deloitte.

department for
children, schools and families

ContactPoint Data Security Review

EXECUTIVE SUMMARY

1st February 2008

This summary is extracted from a full report prepared by Deloitte & Touche LLP ("Deloitte") for the Department for Children, Schools and Families. It sets out the scope and approach to the work performed together with the key findings and recommendations. The detailed findings and recommendations are not included and it does not therefore represent a stand-alone piece of advice. Our report is prepared solely for the Department for Children, Schools and Families and no other party is entitled to rely on our report for any purpose whatsoever. We accept no duty of care or liability to any other party who is shown or gains access to this report.

1 Executive Summary

1.1 Introduction

In December 2007, the Department for Children Schools and Families (DCSF) commissioned Deloitte & Touche LLP (Deloitte) to carry out a data security review of the ContactPoint project.

This document sets out the findings from the security review and provides a number of recommendations, which the department may wish to consider going forward to the next stages of the project.

Background

ContactPoint will be a national database of all children in England, and is part of the wider *Every Child Matters* programme. It will provide a way for people working with children or young people to find out who else is working with the same child. ContactPoint will contain basic information on each child up to their 18th birthday. In certain circumstances, with their explicit consent, a young person's record could stay on ContactPoint up until their 25th birthday. It will also contain contact details for parents and carers and for practitioners and organisations working with a child. It will identify whether a practitioner is a lead professional and/or whether an assessment under the Common Assessment Framework (CAF) exists. It will not be possible to see the CAF itself through ContactPoint, nor any other case or assessment information. The legislative basis for ContactPoint is section 12 of the Children Act 2004 and supporting regulations. The system will be deployed across England to all local authorities, and specific agencies set out in the regulations.

The Senior Responsible Owner (SRO) for the project within the Department for Children, Schools and Families (DCSF) is Tom Jeffery, Director General for Children and Families. A small departmental team with specialist support from WS Atkins, PA Consulting and contractors, is managing the project. In June 2007 the systems development, deployment and hosting was awarded to Capgemini as the primary solution supplier.

Data will be gathered to populate the database from existing information provided by the NHS Patient Records System, DWP Child Benefit database, the Births Register at ONS and the DCSF National Pupil's Database. Data management tools will be used to remove duplicates and cleanse the data from different sources. Once the database is live, it will be refreshed by automated data feeds from the national and local data providers.

No historic practitioner or organisation contact information will be pre-loaded from the four national data sources; instead, this will be created when accessed by Local Authorities and partners via their own case management systems once the system is live. ContactPoint will not hold any child assessment or case information, only whether or not an assessment under the Common Assessment Framework exists.

1.2 Scope & Approach

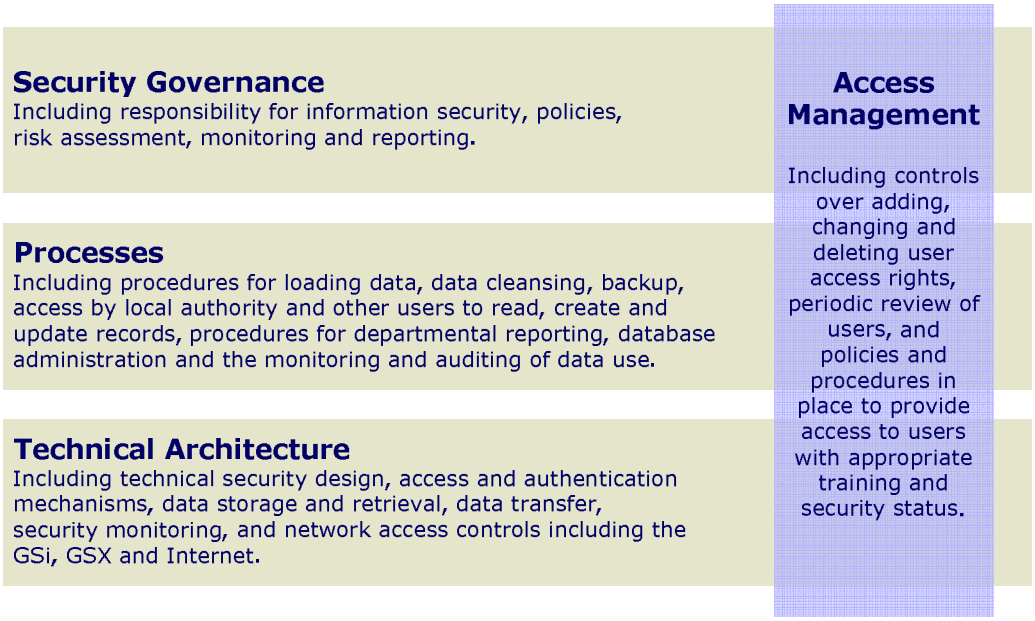
The objective of the review was to provide an independent assessment of the controls in place around the security of citizen data, both during the current development phase and planned for the live implementation of ContactPoint in 2008 and beyond.

We focused the scope of our security review into the following two phases:

1. Security controls over data in use during the development phase of ContactPoint.
2. Security controls incorporated into the design for the deployment and live operations of ContactPoint during 2008 and beyond.

Approach

We categorised our approach across the following four areas to assess data security in each of the two scope phases:



The review was based on interviews with key members of the project team, suppliers and a sample of Local Authorities, observations of current procedures in place, reviews of design documents and of other internal and external assessments that have been performed, and sample testing of the controls that were already in place. Industry 'good practice' including the requirements of ISO27001:2005 (BS7799-2:2005) and the Cabinet Office's Manual of Protective Security (MPS) were used as the basis.

The ContactPoint technical areas reviewed consisted of the following environments:

- Initial Data Load (IDL). This standalone environment is being used to develop and tune matching, cleaning and indexing algorithms on live child data exported from the national data sources of the DWP, NHS, ONS and DCSF in order to increase the level of data quality and integrity within ContactPoint.
- Local Data Quality Tool (LDQT). This web-based tool allows for data submitted from individual Local Authorities and Partner organisation Case Management Systems (CMS) to be tested for quality and compatibility. The system processes the data in memory, without storing it to disk or a database, and provides a score back to the organisation against a set of defined quality criteria allowing them to undertake their own data quality improvement exercises.
- Designs for the planned production environment. At the time of review, the production environment was still in the process of being fully defined, developed and implemented with the project having a target date for the design baseline of March 2008. Therefore, the review only considered the documentation in place and interviewed project team and supplier team members to understand the security elements being planned and designed for the production system.

Following the completion of the review, we have detailed our observations within the following section of this report. The summary overleaf provides a high-level overview of these observations in the context of the overall ContactPoint project environment.

1.3 Key Findings and Recommendations

Conclusion

The importance of information security appears to have been ingrained within the key project areas including:

- people,
- process,
- requirements definition,
- policy development, and
- architectural design.

Security principles, policies and requirements have also been captured, at a high-level, within the contract agreed with the primary supplier for solution delivery and operation.

We do however make a number of recommendations to further reduce the risk that information security will be compromised within the ContactPoint system itself or as a result of misuse of the system by its users. A summary of these recommendations is as follows:

- we recommend that there is clear communication of responsibilities and accountabilities when the governance process is communicated to sponsors and partner organisations;
- we recommend that technical and procedural controls are subject to formal assurance under a recognised standard;
- we recommend that further controls are introduced over the access to data by central system users such as database administrators and report programmers;
- we recommend that processes are defined for the secure disposal of electronic and hard-copy media;
- we recommend that clear guidance about information security matters is provided to all helpdesk staff on the production system.

To implement these recommendations this report sets out a series of additional actions to be taken together with suggested controls that could be designed and implemented beyond those already in place.

It should be noted that risk can only be managed, not eliminated, and therefore there will always be a risk of data security incidents occurring. What is important is that all practical steps to reduce the risk of incidents occurring are taken and when an incident occurs, that it is handled and managed effectively.

Due to the stage at which the project was at when we conducted the review, we recommend that a follow-up review be conducted once the production environment technology and its supporting people, process and procedures are in place.

Security controls for data in use during the development phase of ContactPoint

We have not identified any significant weaknesses in the data security controls implemented for the initial data load (IDL). Through the review of project documentation, conducting of interviews with project team members and physical site visits we determined that the overall level of protection of data transferred to IDL and stored within IDL reduces significantly the risk of a compromise occurring.

We identified a number of minor security failings over how the local data quality tool (LDQT) was being used. The nature of these failings could potentially apply to the production environment and therefore it is recommended that management revisit the level of guidance and support provided to connecting organisations and central support helpdesk operators.

Security controls to be incorporated into the design for the deployment and live operations of ContactPoint

A risk assessment had been carried out by DCSF at the start of the ContactPoint project which followed an informal, but valid, approach, using public surveys available at the time of review such as the DTI security survey 2004, to assess the likelihood and types of possible attack. Although partially updated, the risk assessment as a whole, including threats and likelihood, has not been revisited since its initial completion.

We recommend that the risk assessment be updated on a regular ongoing basis using the formal method associated with the Cabinet Office's Manual of Protective Security (MPS), HMG Infosec Standard No. 1 Issue 3.1. The assessment is likely to identify the need for some additional defence-in-depth controls in addition to those already designed.

Following the risk assessment, formal assurance using a recognised framework should be gained for the security controls and countermeasures required to reduce and manage the identified risks.

The degree of reliance on a hierarchy of self-certifications over a connecting organisation's security processes pose a significant risk to ContactPoint and its assets. This was demonstrated by our limited sample testing at Local Authorities. Whilst a number of retrospective controls such as audits and inspections are planned, the project board should consider the appropriateness of obtaining formal independent assurance and accreditation of the supporting security operating procedures at connecting organisations before allowing connectivity or sponsorship. This will be of particular importance where sponsoring organisations (Local Authorities and National Partners) lack the internal expertise or resource to effectively verify and monitor their own compliance and that of their partner organisations. It is appreciated this could be a material overhead to the operation of ContactPoint. Accordingly, the project board should consider up-front accreditation for connecting organisations posing greater risk, with assessments of other organisations carried out over time. Compliance should be re-validated on a regular basis such as annually or two-yearly depending on risk.

In addition, during the development of the detailed guidance for connecting organisations, detailed data handling procedures should be included. These procedures should cover both electronic and hardcopy information that may be directly or indirectly associated with the ContactPoint system over its entire life cycle.

While the ContactPoint team can design strong controls into the system and provide good advice to connecting organisations, there is a limit to their ability to enforce good practice or to monitor incidents and control breakdowns. We recommend that the DCSF participate in government-wide security initiatives to maintain and enhance roles, responsibilities and accountability for the security of systems such as ContactPoint that extend across multiple Departments and other organisations. These initiatives could help to define methods for effective sanctions for non-compliance or incidents.
