Deloitte.

department for
children, schools and families

ContactPoint Data Security Review

FINAL REPORT

1st February 2008

Contents

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

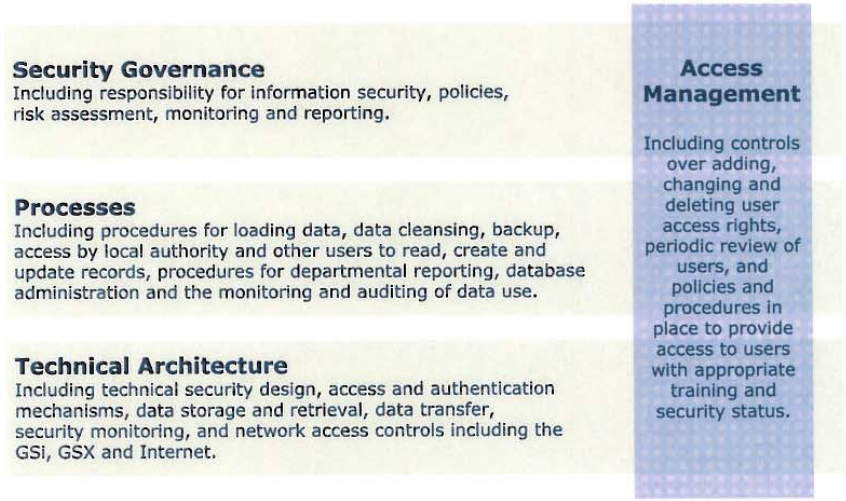
The objective of the review was to provide an independent assessment of the controls in place around the security of citizen data, both during the current development phase and planned for the live implementation of ContactPoint in 2008 and beyond.

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.

2 Observations

In our executive summary we describe the importance that we observed being given to information security throughout the project. We have however noted a number of residual risks regarding information security within ContactPoint:

- There is a risk to the effectiveness of overall security governance due to the lack of effective responsible ownership and accountability across all stakeholders and connected organisations for data.
- There is a risk that the technical and procedural controls will not be effective at providing the required level of protection as they have not been formally assured to a recognised standard.
- Risks associated with the accidental leakage of data could be reduced by introducing further controls over the access to data by central system users such as database administrators and report programmers.
- The Data lifecycle is not fully defined. In particular the risk exists that lack of defined processes around the disposal of electronic and hard-copy media could lead to information leakage.
- There is a risk of inappropriate advice being provided to connecting organisations by the central support helpdesk resulting in security practices not being followed or by-passed.

The observations in this section describe the background to these risks and include our recommendations for additional controls to mitigate these risks.

2.1 Asset valuation and information classification

Observation

A good information risk management process starts with the identification of the assets within scope, such as child data in this case, and puts a value on these assets based on the potential business impact that would result if the asset's confidentiality, integrity or availability were to be compromised. The 'business' could be the ContactPoint project, the DCSF, Government or UK as a whole depending on the context. Based upon the determined level of impact if the asset were to be compromised, it will be given a value or, more commonly, a classification as an abstract representation of value.

The ContactPoint project's risk assessment documentation includes a high-level identification of twelve key data asset groups. It also provides a four-point scale for impacts to these assets using the Cabinet Office's e-Government Interoperability Framework (e-GIF) Authentication Framework impact definitions, based upon consultation with DCSF and local authority Trailblazer teams. For example, in the assessment over half the asset groups have been given the highest impact rating possible for the compromise of confidentiality, and a similar number for integrity.

The project has not assigned a formal value or classification to these data asset groups which is not in line with good practice, including the Cabinet Office's, ISO17799:2000[1] aligned, Manual of Protective Security (MPS). The main rationale provided for this approach was to provide the project the freedom to design customised security controls specific to the threats to child data.

In addition, we observed a perception within the project that end-users of the system would need to have a formal level of HMG security vetting if MPS Protective Marking was to be

[1] ISO17799:2000 has been superseded by ISO27002. In view of the fact that the text of the new standard is mostly, but not entirely unchanged, the references to ISO/17799:2000 remain in the Manual of Protective Security.

adopted and that for a large proportion of the end-user population and their organisations this would not be practical. Therefore, the project has designed specific personnel controls for example, enhanced Criminal Records Bureau Checks, tailored security training and need-to-know. While these controls are not formally based upon or benchmarked against the MPS suggested HMG Baseline Personnel Security Standard, they are close to the Standard and in certain areas exceed this for specific threats to children.

It should be noted that a large number of the security controls and countermeasures that have already been designed by the ContactPoint project match the standard that we would expect to see implemented for data with a formal classification under the Protective Marking scheme as defined within the MPS.

Recommendation

The MPS is a code of practice applicable to all central government departments and is to be regarded as a starting point for developing organisation specific security guidance. It specifically states that not all of the guidance and controls in it may be applicable or, furthermore, additional controls not included in it may be required. For example, it gives definitions of increasing classifications[2] of data, based on business impact in the Government context, and guidance for the approaches to be taken when handling and protecting such data, whilst allowing each organisation to make their own risk based judgements for their particular situation.

We recommend that information assets within ContactPoint be classified based on the MPS definitions. In addition MPS should be followed by the project as a baseline guidance with additions as appropriate for child data. The precise business impacts, and therefore classifications, are a matter for the department to decide based on their judgement. However we would expect that the majority of the data within ContactPoint to attract a RESTRICTED classification. Certain data assets may be classified at lower markings like PROTECT or the higher marking of CONFIDENTIAL, depending on what is actually stored or transferred and the volume managed. For example, shielded child data and system data associated with security functions such as authentication, authorisation and audit logging might be classified as CONFIDENTIAL.

The ContactPoint project risk assessment documentation gives a higher business impact for bulk child data, compared to very small volumes of child data. We recommend that bulk volume data, including archives and backups, continue to be treated as having a higher business impact and therefore higher resulting asset classification.

The HMG Baseline Personnel Security Standard follows good HR practice for commercial as well as government organisations. We recommend that the ContactPoint end-user personnel vetting requirements are formally based upon the HMG Baseline Personnel Security Standard and the specific requirements above this for threats to children are maintained. By using a recognised standard as the basis for the minimum personnel requirements there will be less room for misunderstanding of the level and quality of vetting checks required across the different government and non-government organisations involved to access the classified data within ContactPoint.

[2] MPS defines the following data classifications, known as Protective Markings, aligned to HMG impact levels (ILs) – PROTECT (not a formal marking, IL 2), RESTRICTED (IL 3), CONFIDENTIAL (IL 4), SECRET (IL 5), TOP SECRET (IL 6). See Appendix A for definitions of Protect, Restricted and Confidential.

2.2 Ongoing risk assessment

Observation

The ContactPoint project initiated a high-level risk assessment in October 2005 that was issued in June 2006. This risk assessment followed an informal, but valid, approach and used public surveys, such as the DTI security survey 2004, to assess the likelihood and types of threats that could arise. The countermeasures and resulting residual risks sections of the risk assessment were updated in May 2007 to align with the technical controls from the detailed design exercise.

The risk assessment as a whole, including threats and likelihood, has not been revisited since its initial completion. Security good practice advocates the continual need to review and update risk assessments in line with the continually changing threat landscape.

In addition, this high-level risk assessment does not take into account specific technical vulnerabilities that may exist within the proposed technical solution elements, such as a bulk file transfer server, because it has been conducted prior to the detailed design being completed.

Recommendation

We recommend that the risk assessment be updated on a regular, ongoing basis and be revised to follow a formal method. Given our observation 2.1 above, the approach contained within HMG Infosec Standard No. 1 Issue 3.1, a supplement to the MPS, is recommended. This standard will also give the added advantage of providing a formal threat modelling approach.

2.3 Formal assurance of countermeasures

Observation

The security countermeasures identified within the risk assessment to manage the risks to assets have not had a formal assurance level placed upon them. Whilst some of the technical controls have had e-GIF assurance levels assigned to them in supporting documentation it is not clear how these map back to the risk assessment or how they will be formally assured and verified within the ContactPoint implementation.

It is common for security controls to undergo a level of formal assurance to ascertain their effectiveness and from this to determine the level by which the residual risk is reduced. Common Criteria, ISO 15408, is a widely recognised method for achieving this both within the UK and internationally. The criteria prescribe a number of degrees of rigour known as Assurance Levels and certificates are usually issued by the scheme certification body for controls meeting the requirements for a claimed level of assurance. It is possible to obtain assurances over operational processes and procedures in addition to technical controls.

Without formal assurance of the security control countermeasures, it is not possible to have a high level of confidence over the residual risk to the system.

Recommendation

We recommend that the security controls and countermeasures be formally assured using a process such as Common Criteria or equivalent. As well as the technical controls being evaluated, this should include the assurance of the supporting operating procedures and processes, using a scheme like the CESG Tailored Assurance Service. The scope of procedural and process assurance should as far as possible include the proposed framework under which organisations will be allowed to interact with ContactPoint both directly and indirectly (see 2.5).

2.4 Project assurance function

Observation

The ContactPoint project was intended to follow the Prince2 project management methodology. The project organisation is defined and all members of the project board and team appear to have a clear understanding of their roles and responsibilities.

Our review identified that within the ContactPoint project organisational structure provision for an independent project assurance function had not been fully defined. To date, the project board has been heavily reliant upon technical assurance provided from within the project delivery teams themselves. These teams:

- identify technical requirements,
- design solutions to meet the requirements,
- review the appropriateness of the requirements and solutions, and
- approve the requirements and solutions.

This is particularly true of the security policies and procedures due to the specialist nature and understanding required to provide assurance.

For security this situation was exacerbated by the department's limited maturity in the area of information security at the time of key project security decisions being made. The department only set up a Departmental Security Unit (DSU) and appointed a Departmental Security Officer (DSO) in early 2007 and an Accreditor in mid 2007. Prior to this there was a very limited IT security function within CIO Group made up of a single individual for DfES. In addition, we observed Internal Audit had limited capability and involvement in projects.

It is a credit to the strength of external security resources within the ContactPoint project delivery teams that the level of security designed is at the level it is given the lack of strong independent technical assurance and oversight. However, there is always the risk that "you don't know what you don't know" and the benefits of having good independent project assurance cannot be underestimated.

In addition, we observed that change control processes have been developed and implemented in support of ContactPoint system development. The current change processes require system change requests to be approved by a dedicated Change Control Board (CCB). The CCB consists of key members of the project delivery team and is ultimately responsible for approving all system change requests.

Whilst it is positive to see defined change control processes, we identified that no assurance has been obtained by DCSF regarding the operational effectiveness and robustness of these processes or their alignment to recognised industry good practice and standards, including CCB membership.

Recommendation

It should be noted that at the time we started our review a new programme based organisation structure was put in place that incorporated the ContactPoint project, among others, focusing on sharing resource expertise and centres of excellence across projects. This new structure appeared to address a number of the general shortcomings in the project assurance area; however, it was not embedded and operating at the time of our review. Therefore, we recommend that the project board consider putting in place a formal independent project assurance function for the ContactPoint project. This function should be separate from the project delivery teams and could be provided by other areas of DCSF such as specialists from CIO Group, DSU and Internal Audit.

In addition, we would recommend that the ContactPoint project board review the change control processes, including the membership of the CCB, to confirm that recognised good practice principles have been adopted and are appropriately implemented and monitored.

2.5 Assurance over, and accountability of, connecting organisations

Observations

Self certification and devolved user administration

Our review highlighted that guidance and tools have been developed, and are in the process of being developed, by the ContactPoint project team to support organisations wishing to connect to ContactPoint in-line with the applicable legislation. Given the number of organisations required to connect over a relatively short period the project has taken a devolved approach with organisations self-certifying that they comply with the ContactPoint guidance, including security policy. In addition, a Local Authority or National Data Provider can then provide onward connections and sponsor Partner organisations, such as charities and GP practices, which in turn self-certify to the sponsoring organisation. For example, through the LA Readiness Assessment (LARA) tool checklist a Local Authority is asked whether or not it has a user training plan in place for ContactPoint and that users have had the necessary vetting checks. A Partner organisation, such as a local charity, will then answer these same checklist questions posed to them by their sponsoring Local Authority.

The accountability for verification of assessments and ongoing monitoring lies with the Director of Children's Services at Local Authorities and the equivalent director in a National Organisation as prescribed by enabling legislation. These accountabilities are reflected in the draft accreditation blueprint. The risk remains that these sponsoring organisations lack the expertise or resource to adequately verify and monitor security compliance. ContactPoint does not require independent verification of the answers and evidence provided by the Local Authority or sponsored Partner prior to them connecting.

In addition, the provisioning of users into ContactPoint is achieved at a technical level using federated identity trusts from each of the connecting organisations. Whilst technical and procedural security requirements surrounding these have been defined at a high-level, it is not clear how assurance over what is implemented and operated in practice will be achieved. Therefore, there is potentially significant reliance on the local processes and procedures for managing access to ContactPoint as a whole.

Assessment of Case Management Systems

The only exception to self-certification is that the organisation's Case Management Systems (CMS) must pass technical interoperability and data quality tests by passing a set of criteria in a ContactPoint managed test environment. The ContactPoint project team will not be providing direct technical support to connecting organisations that will need to liaise with their existing CMS and IT suppliers.

Lack of guidance for handling data to be loaded into ContactPoint

During our review we observed that, whilst guidance had been provided to Local Authorities defining how the Local Data Quality Tool (LDQT) should be used, the guidelines did not extend to security and management of data extracted from local Case Management Systems (CMS) prior to upload to the LDQT. The ContactPoint team had placed reliance on the effectiveness and adequacy of the Local Authorities existing controls and processes to ensure extracted data was sufficiently secured and restricted.

From our sample testing we identified that in all cases live data exported from the local authorities systems for ContactPoint, but prior to upload and handover to ContactPoint, was at risk of compromise. In addition, we observed that the security guidance that had been provided to the local authorities was not being followed. For example, in one instance an

organisation was sharing the same single user certificate to LDQT for all of their users (see 2.9).

Recommendations

Reconsider the guidance provided for handling ContactPoint related data

We recommend that the project team reconsider the controls that connecting organisations need to assure the secure treatment of data being loaded or updated in ContactPoint. The project team should look to extend the guidance already provided to connecting organisations and define a minimum level of data security and control that should be employed when handling or processing ContactPoint related data.

Introduce risk-based assessments of connecting organisations' security

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.

For example a large charity requiring access to ContactPoint might be subject to up-front accreditation while a recently audited Health Authority, with regularly monitored procedures in place to handle sensitive information, might initially self certify.

In order to provide the scalability required for the potentially large number of ContactPoint connecting organisation accreditations and follow-up audits we recommend that the project consider implementing a formal scheme, or negotiate extending an existing one, to provide a framework for auditors to be trained, certified and registered with ContactPoint. The scheme would include a supporting toolkit and could include auditors from within Government and private sector. Similar schemes already operate across Government, Connecting for Health and the private sector such as:

- the CESG Listed Advisor Scheme (CLAS),
- BSI Lead Auditor,
- Payment Card Industry Qualified Security Assessor, and
- regulated external audit firms.

Such audits should where possible and practical be linked to and extend existing regular audit and accreditation processes that connecting organisations already have in place so as to minimise duplication of effort and resource impact for the connecting organisations.

Participate in cross government data security initiatives

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. The use of a modelling approach such as RACI (Responsible, Accountable, Consulted and Informed) would help to achieve this.

2.6 Data handling and destruction

Observation

It was evident from our review that security procedures and guidelines had been created by the ContactPoint project team for use by departmental staff and their supplier for the development phase of the project. For example, a number of these procedures and guidelines specifically related to the processes that governed Initial Data Load (IDL) and Local Data Quality Tool (LDQT) activities. In addition, at the time of our review the ContactPoint project team were still developing good practice procedures and guidance for the production system for use by connecting organisations such as Local Authorities and partners.

From our review and testing of IDL specifically, we observed that the ContactPoint project team and supplier have handled all data extracts in accordance with the IDL security procedures and guidelines. Data provided for IDL by the four national data providers was found to have been transferred and stored in accordance with the defined security procedures and guidelines with the potential risk of any data compromise significantly reduced.

However, we identified that procedures and guidelines relating to the destruction or decommissioning of sensitive data/media by either the ContactPoint project, supplier or connecting organisations following the completion of IDL and other development activities, such as LDQT, had not been fully documented. At the time of our review procedures for the production system operations were still to be developed.

There is a risk that media no longer in use that contains residual ContactPoint data is not disposed of correctly and ends up being reused by another party. For example there have been a number of cases at other organisations where second-hand / refurbished computer hard drives from desktops, laptops, servers and storage area networks have been privately purchased on auction websites and found to contain the previous owner's data.

In addition, through review of the documentation that was still in development by the ContactPoint team we identified that guidance relating to the management and handling of hardcopy information had been omitted from the initial procedures and guidance provided to the connecting organisations. Whilst there are technical controls to limit the extracting and reporting of child data from the ContactPoint system it is still possible in a number of legitimate cases. For example detailed audit reports will be generated by the live system for review and analysis by Local Authority/Partner 'User Managers' for the purposes of identifying evidence of system misuse. Whilst this report will not contain specific child data, the contents of this and other reports should be considered as sensitive and appropriate guidance should be provided to support the appropriate safe management of this information.

Recommendation

We recommend that the existing data handling procedures, and those in development for production, be updated to include specific guidance for the destruction of both electronic and physical media that have contained ContactPoint child and operational data. We suggest that the ContactPoint project team consider MPS supplement HMG Infosec Standard 5 "Secure Sanitisation of Protectively Marked or Sensitive Information" and its supporting guidance, Manual S, as the basis for the updated destruction guidance.

In addition, the ContactPoint project team should develop detailed handling procedures for use by connecting organisations. These procedures should cover both electronic and hardcopy information that may be directly or indirectly associated with the ContactPoint system. An example of indirectly associated data would be data that has been prepared as an export from

a CMS by a Local Authority for submission to ContactPoint but which has yet to be submitted to ContactPoint.

Support contractors and engineers, with particular attention to those operating during out-of-hours incidents, should be included within the scope of the procedures to reduce the risk of cases such as faulty media being removed, repaired and sold-on as refurbished.

2.7 Shielded Record and migrated data testing requirements

Observation

As part of our review, we investigated the testing of shielded records within the development and production environments. Access to shielded records should be restricted on a strict 'need-to-know' basis. We established that the data sent by the national data providers as part of IDL contained both shielded and unshielded records, intentionally without distinction, and that this data was loaded into the IDL environment, in accordance with IDL procedures and guidelines, to enable testing of the ContactPoint solution's complex data-matching algorithms. These algorithms are used to link data records from each of the national data providers to an individual child with a high probability of match accuracy.

The IDL data and tuned algorithms will be migrated to the production environment. An additional data feed from the national data providers with changes since the IDL will then be applied to the database, but with shielded records flagged, prior to user acceptance testing and go live. At the time of our review the testing procedures for the migration did not cover validation of shielded record flags being correctly applied retrospectively from the additional data feed to the IDL data.

At the time of our review user acceptance testing criteria for shielded records and associated functionality had not been developed.

Recommendation

We recommend that the ContactPoint project team seek to gain assurance over the data matching algorithms ability to securely and correctly process shielded records.

In addition, assurance should be sought that the migrated records without shielding flags will be correctly flagged as shielded in the production environment.

2.8 Protection and separation of sensitive data within the database

Observation

An integral part of our review was to assess the ContactPoint system's architecture design and technical environment. This aspect of the review included analysis of initial technical design documentation and discussion with key members of the ContactPoint project team. It should be noted that at the time of our review the detailed technical design was still being worked on and the production environment was not physically in place.

MATERIAL WITHHELD; EXEMPT UNDER SECTION 31(1)(a) OF FREEDOM OF INFORMATION ACT 2000.

Database administrators and system operators have the highest level of access to the ContactPoint databases. This level of access will permit access to all aspects of the database including child, archive, reporting, authentication and audit log data. They have the ability to view, modify and extract data records directly from the ContactPoint databases. We understand that there is a valid requirement for database administrators to have privileged access to the databases and that additional security controls are to be implemented to further reduce the associated risks. However, we note that there is still a potential risk that a database administrator will have the ability to view and extract data directly from the databases either intentionally or through human error. Whilst segregation of duties is covered in the project security documentation reviewed, it does not go to the level of detailed required to protect from this threat.

Recommendation

The ContactPoint project team should consider the implementation of additional defence-in-depth controls to enforce segregation of duties and other checks and controls such that the risk of unauthorised data leakage and modification from operators and database administrators is reduced. The level and type of additional controls should be determined as

[3] Children and their associated records are moved from the child database to the archive database when they reach the age of 18, unless meeting certain criteria in which case they will be moved when they are 25. A record is generally removed from archive after 6 years.

part of the updated risk assessment discussed in 2.2. Examples of additional controls might include:

- the use of separate database systems with different administrators for the different databases,
- the use of encryption for certain types of data,
- integrity checks to detect changes or corruption to the databases,
- additional levels of staff vetting such as Developed Vetting for administrators, and/or
- process changes to introduce more dual-control and "four-eyes" checks.

Additional controls to protect from the threat of hackers attacking and bypassing the application level controls should also be considered.

2.9 Local Data Quality Tool guidelines and support

Observation

During our review, we investigated the use of LDQT within Local Authorities. As ContactPoint is still in the development phase, many Local Authorities are using LDQT to test and validate compatibility of data extracted from their local Case Management System ("CMS") with the ContactPoint system. We observed that a series of security controls have been implemented to secure the use of LDQT, for example, communication encryption and user authentication. We established that Local Authority users are all required to receive training and guidance in the use of the LDQT before access to or use of the tool is permitted.

Through onsite review with a sample of Local Authorities, we identified that sensitive data is being exported from local CMS and stored on network file shares prior to being uploaded to the LDQT for testing and validation. No formal guidelines have been provided by the ContactPoint project team specifying a minimum level of security control for the management and handling of CMS extract data prior to import to ContactPoint.

In addition, we noted instances where a Local Authority team were sharing a single digital certificate for all users to access the LDQT environment due to their IT teams having difficulty in getting other certificates loaded on to their PCs. When contacting the central LDQT helpdesk for support the Local Authority was advised to continue their current certificate sharing practice. Sharing of certificates reduces non-repudiation and the accountability within the system.

Recommendation

Additional guidance and support should be provided to users and local administrators of the LDQT environment in order to comply with the ContactPoint security requirements.

ContactPoint should investigate the level of training provided to the central LDQT support helpdesk operators on the security requirements of the system and the quality of security advice provided to Local Authorities by them.

Whilst it is recognised that the security of data held within Local Authorities is not a direct responsibility of ContactPoint project team, exported CMS data is being used during the course of work for the ContactPoint project. If there were a compromise or accidental disclosure of this information there would be the potential for negative reputational impact to the wider ContactPoint project. See observation 2.6 for further detail on recommendations for data handling.

Appendix A – Classifications

The following definitions of PROTECT, RESTRICTED and CONFIDENTIAL are based on the August 2007 edition of the Manual of Protective Security; they are not a complete list of all classifications in the Manual. The definitions below are for determining asset value based on the consequences of a compromise. More detailed information on impacts and baseline levels of protection is contained in the Manual and HMG Infosec Standard No. 1 Issue 3.1 supplement. An asset does not need to match all statements to be assigned a classification.

The compromise of assets marked **PROTECT** would be likely to:

- Cause substantial distress to individuals
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and or/the e-government Security Framework).

And, depending on the severity of the circumstances:

- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Disadvantage government in commercial or policy negotiations with others

The compromise of assets marked **RESTRICTED** would be likely to:

- adversely affect diplomatic relations
- cause substantial distress to individuals
- make it more difficult to maintain the operational effectiveness or security of UK or allied forces
- cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies
- prejudice the investigation or facilitate the commission of crime
- breach proper undertakings to maintain the confidence of information provided by third parties
- impede the effective development or operation of government policies
- breach statutory restrictions on the disclosure of information (except the Data Protection Act - which can be addressed by other impact statements and/or the e-Government Security Framework).
- disadvantage government in commercial or policy negotiations with others
- undermine the proper management of the public sector and its operations

The compromise of assets marked **CONFIDENTIAL** would be likely to:

- materially damage diplomatic relations, that is, cause formal protest or other sanctions
- prejudice individual security or liberty
- cause serious damage to the operational effectiveness or security of UK or allied forces
- cause serious damage to the effectiveness of valuable security or intelligence operations
- work substantially against national finances or economic and commercial interests
- substantially undermine the financial viability of major organisations
- impede the investigation or facilitate the commission of serious crime
- seriously impede the development or operation of major government policies
- shut down or otherwise substantially disrupt significant national operations

Statement of Responsibilities

We take responsibility for this report which is prepared on the basis of the limitations set out below. The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that may exist or all improvements that might be made. Any recommendations made for improvements should be assessed by you for their full impact before they are implemented.

Deloitte & Touche LLP

London

February 2008

In this document references to Deloitte are references to Deloitte & Touche LLP.