DATA SECURITY

REPORT

SEPTEMBER 2009

TABLE OF CONTENTS

TABLE OF CONTENTS 3

SECTION ONE ~ INTRODUCTION 5

SECTION TWO ~ SUMMARY OF RECOMMENDATIONS 7

Risk……7
Organisation 7
Consistent policies 7
Change and approach 7
Caution 8

SECTION THREE ~ FINDINGS OF THE REVIEW 9

Introduction 9
General observations 9
Organisation 9
Establishment of policies 11
Quality assurance 12
Variations in practice 12
Variations in practice: staff issues 13
Variations in practice: systems 14
Variations in practice: security processes 16
Department of Health and Social Services 16
Department of Education Sport and Culture 18

SECTION FOUR ~ IMPLICATIONS 20

Risk……20
Organisation 20
Consistent policies 21
Change and approach 21
Caution 22

APPENDIX ONE ~ TERMS OF REFERENCE 24

SECTION ONE ~ INTRODUCTION

1. In recent times public attention has been attracted to alleged failures of the United Kingdom Government to safeguard the information that it holds concerning both its own activity but also individual citizens. This public attention has led to a series of enquiries and to wide ranging action led by the Cabinet Office to improve data security.

2. In general, the steps taken by the United Kingdom Government to improve data security have not been replicated within the States. This is in part due to the fact that there has not been a parallel within the Island to the incidents which have given rise to such public concern on the mainland of the United Kingdom. However, in view of the significance of this issue, and after consultation, it seemed appropriate to commission a review into data security within the States.

3. Data security matters for at least two reasons.

4. Firstly, information about people, if misplaced, can be used by the unscrupulous to take advantage of any individual and, in particular, the vulnerable and disadvantaged. With the development of technology, the risk that information has been misplaced and, possibly, abused can exist without any of the people concerned being aware of the risk to them until the consequences become evident.

5. Secondly, as this risk of abuse becomes more widely known, so people will become more distrustful of the government which exists to serve them. This could corrode the relationship of trust between a government and citizens which is an important foundation of effective administration.

6. Accordingly, I commissioned PricewaterhouseCoopers LLP (PWC) to undertake a review specifying terms of reference which are set out in Appendix One to this paper.

7. The review was undertaken in two stages.

8. The first stage consisted of a review of States-wide arrangements and practices. The second stage of the review consisted of a series of more detailed reviews of practices within individual departments including: Income Tax, Health and Social Services,

Housing, Judicial Greffe, Social Security, and Education Sport and Culture. Reviews were also carried out of practices within certain central units including the Information Services Department, Human Resources Department and Jersey Property Holdings.

9. As can be seen from the terms of reference, the review was not limited to the security of data held in electronic media. Issues concerning the physical security of information held on paper were also considered.

10. The purpose of this report is to set out the outcome of the review and is based on an outline report of detailed findings which has been submitted to me by PWC.

11. In Section Three of this report, I will set out a list of the principal findings of the review. This list includes all of the generic issues that have been raised. These are based on detailed findings in respect of the individual departments examined which have been discussed with the relevant people within the departments concerned. As will be seen, however, in one or two cases, the issues raised in respect of individual departments appeared of such significance that they should be mentioned in this report and they are also included in Section Three.

12. The pattern of practice within the States uncovered as a result of the review raises questions about the organisational arrangements within the States. These implications are examined in Section Four of this report.

13. I am grateful to PWC for the work which they undertook and for the willing assistance and co-operation of the large number of staff of the States who co-operated in this work.

14. A summary of the outcome of the review is set out in the following section of this report.

SECTION TWO ~ SUMMARY OF RECOMMENDATIONS

Risk

15. Although there are examples of good practice within the States, the nature and extent of the variations in practice uncovered by the review suggests that the States are not consistent in following best practice in safeguarding the security of data.

16. One consequence of this is that there must be a significant risk that, sooner or later, the States will suffer the sort of data security failure that has occurred on the mainland.

Organisation

17. The variations in practice uncovered by the review undoubtedly flow in large part from the organisational arrangements for managing the States' network and safeguarding data security.

18. Responsibility for managing data security is one of the responsibilities of a department's chief officer. Where a department is large enough to support an active data security manager, some appropriate safeguarding steps may have been and indeed, as the review has shown, have been taken. However, even where major departments have the resources to support some data security arrangements, practice and effectiveness will vary.

Consistent policies

19. If follows from these comments that it is most unlikely that, under current arrangements, the States:

    (1) Will proactively develop a comprehensive set of data security policies, and

    (2) Ensure that they are applied consistently and reliably on a States-wide basis

Change and approach

20. To correct this state of affairs:

(1) It is important that the risk of loss or abuse of information held by the States is prevented and, in particular, that proper security policies and practices are implemented throughout the States, without significant variation.

(2) Maintenance of data security should be the clear responsibility of an officer with a States-wide remit. Such a person may be the States' Chief Information Officer.

(3) This officer should have responsibility for the following matters in particular

(a) Ensuring that there is a comprehensive map of data held within the States.

(b) Ensuring that there is a comprehensive assessment of the risks to the security of data held by the States which is refreshed on a regular basis.

(c) Ensuring that a comprehensive set of policies is established to manage the risks to the security of data held by the States.

(d) Ensuring that departmental compliance with these policies is monitored on a regular basis.

(e) Ensuring that appropriate corrective action is taken where monitoring demonstrates that unacceptable variations in practice have occurred.

21. There should be no tolerance for departments which derogate from States-wide policies. Although circumstances may and indeed will vary between departments, it is important that such variations are not used to excuse variations from the practices required by the States. It should therefore be incumbent upon Chief Officers to identify cases in which some variation from States-wide policies may be necessary and to agree the appropriate action with whoever becomes responsible for States wide management of data security.

Caution

22. Even if all of these steps are taken, it will not be possible to eliminate all possibility of data security failures. Perfection is not an achievable idea.

23. This should not be an excuse for not taking action. The aim should be to ensure that all reasonable steps are taken to eliminate security failures so that any breaches do not result from the States' inaction and inconsistency.

SECTION THREE ~ FINDINGS OF THE REVIEW

Introduction

24. The purpose of this section of the report is to set out the detailed findings of the review. These are set out under a number of sub headings:

    (1) General observations;

    (2) Organisation;

    (3) Establishment of policies;

    (4) Variations in practice; and

    (5) Security processes.

25. As I have indicated above, in two instances issues were identified that appear of such significance that they should be mentioned separately. These concern the Health and Social Services Department and the Education, Sport and Culture Department and are set out at the end of this Section.

General observations

26. It is important to note that the review identified that there are many areas of good practice within the States. A considerable amount of work has been done and commitment shown by many members of the staff of the States in establishing good practice and thus in securing the security of data held by the States about the people of the Island.

27. However, in spite of this work, as will be seen, the performance of the States in this area is inconsistent.

Organisation

Findings

28. Within the States, there is no central executive authority for management of information held by the States. Data, where held, is 'owned' by the individual departments within which that information is held. Each department's Chief Officer is responsible for data

security. To assist Chief Officers to discharge this responsibility, a number of standards have been developed by the Security Policy Group (SPoG) which consists of officers representing States departments.

29. The fact that information is owned by departments individually is reflected in the fact that departments have individual registrations with the Office of the Data Protection Commissioner.

30. Whilst each department is intended to have appointed a Departmental Information Security Administrator (DISA), in practice only the larger departments have the resources to appoint staff dedicated to this function. In smaller departments, the role of DISA will be discharged by individuals as one of many responsibilities. In any event, the role of DISA is very limited. In most cases it is limited to being a systems administrator although in larger departments, there additional resources covering data security.

31. In view of the lack of a central executive authority, it is perhaps unsurprising that there is no data map covering all data held by the States wherever it is held. Nor are there data security risk assessments either prepared centrally or locally.

Consequences and risks

32. The absence of a central executive authority means that:

(1) there will be variations in security practice between the larger and smaller departments and, probably, within departments. These will result from differences between the resources available in different departments and between the extent of the understanding of different departments of the scale of potential risks.

(2) no-one centrally is in a position to know what information is held by the States, where it is held, by whom it is held and for what purpose.

(3) no-one centrally is responsible for identifying variations in practice that may lead to significant risks to the security of data held by the States.

(4) no-one centrally is in a position to take or require that others should take the action necessary to manage and eliminate risks to the security of data held by the States.

33. In short, management of risks to the security of data held by the States depends upon the vigour with which individual departments take action to deal with the risks and their individual understanding.

Establishment of policies

Findings

34. The States have established a number of policies concerning the management of the States network and in particular the management of information held within that network. This has been done through the SPoG which includes representatives of the principal departments of the States.

35. However, the policies that have been developed have responded to concerns identified and expressed by individual departments (i.e. they have not been based on comprehensive data maps or comprehensive data security risk assessments since none exist). Moreover, the standards do not necessarily take account of all relevant external developments. For example, the review found that the States have not assessed compliance with the Payment Card Industry Data Security Standard: a recently established industry standard that deals with the way in which suppliers (in this case the States) should deal with credit card payments.

36. Inevitably, therefore, the policies developed by the SPoG do not necessarily represent a comprehensive set of policies covering all of the principal risks.

37. Moreover, a number of the policies established have passed their review date:

(1) Acceptable use of e-mail.

(2) The information security personal handbook.

(3) DISA roles and responsibilities.

(4) Remote access.

(5) Remote access supplier assessment.

Consequences and risks

38. The consequence is that even if departmental Chief Officers are well-informed and committed to safeguarding data security, they cannot rely upon the States' guidance on how this should be done being either comprehensive or up to date.

39. The result is that better resourced departments will be obliged to develop their own practices which they will be disinclined to change if the States subsequently develop States-wide guidance. This leads to:

    (1) duplication of effort between departments developing their own practice to supplement States-wide guidance;

    (2) variations in practice between better-resourced and smaller departments;

    (3) departments regarding States-wide guidance as subordinate to departments' own practices.

40. These observations should not be taken as criticisms of the members of staff who have served on the SPoG. The risks inherent in the current arrangements appear to follow from the organisation, position and the terms of reference of SPoG rather than from the way in which it has worked.

Quality assurance

Findings

41. Perhaps unsurprisingly, there are no formal compliance and assurance programmes to assess whether data security policies are being followed consistently throughout the States. This is a matter within the responsibility of individual department Chief Officers.

Consequences and risks

42. The result is that significant variations in practice are unlikely to be identified or corrected.

Variations in practice

43. The variations in practice identified by the review are set out below and grouped under three headings:

(1) Staff issues.

(2) Systems.

(3) Security processes.

Variations in practice: staff issues

Findings

44. It seems clear that there are within the States' staff different levels of awareness of the States' data security policies and of where they may be found if staff need to refer to them.

45. Some departments cover data security in induction training but others do not provide mandatory training. There is a States-wide learning and development directory of courses but no information security courses are listed.

46. Job descriptions for States staff do not all have appropriate references to data security and confidentiality. Moreover, data security does not appear always to be covered in performance review and appraisal processes.

47. All civil servants are required to sign an official secrets declaration before commencing their employment. When the declaration is signed, full details of the applicable law are provided for reference (although not full details of the States' data security policies). This information is in small print and no summary detail is provided. There is a risk that this will not be read fully by staff.

48. As departments make use of the services of people who are not themselves employees of the States (e.g. agency staff within the Department of Health and Social Services) it is important that steps are taken to ensure that agency or contracted staff comply with the States' normal policies with regard to data security. This does not appear to be done consistently. For example, the Department of Health and Social Services does not appear to monitor the procedures of agencies providing agency staff for vetting and training staff.

49. As further examples, the Housing and Social Security Departments have external information technology suppliers whose people have permanent access to live systems. This access and the suppliers' staff's compliance with the States' data security requirements are not monitored.

Consequences and risks

50. It is fundamental to safeguarding the security of data that all of the people employed by the States in any capacity understand the States' policies and practices and the importance of complying with them. A failure in this respect heightens the risk that people unwittingly deal inappropriately with data. In particular, they may not understand the risks that they are dealing with and how to deal with them.

51. These disciplines should apply to all people who work for and within departments: including agency staff. Unless data security responsibilities are made clear one cannot expect that all will know of the States' policies or respect them.

Variations in practice: systems

Findings

52. The hard discs of lap tops and personal computers used by staff within the States are not routinely encrypted (i.e. unauthorised people could scan and downloaded data without having access to the means to decrypt the data).

53. Access to writeable drives, such as for CDs or DVDs are not routinely disabled (i.e. it would be possible in large numbers of cases to download copies of data to transportable media such as CDs or DVDs. Since hard discs are not routinely encrypted, the facility of downloading is obviously dangerous).

54. There are policies governing the use of USB portable media devices but there are no physical restrictions to prevent their usage (e.g. the disabling of USB ports).

55. In the Department of Employment and Social Security, eight members of staff can access the BACS[1] file and it is not 'read only'. The BACS file is the file which retains

[1] Banks' Automated Clearing System.

information about the banking details of people receiving Social Security benefits.[2] It would be normal practice to restrict access to such a file to the smallest number of people possible and to monitor the use of such access. The fact that the file is not 'read only' leaves open the possibility that members of staff accessing the file might be able illegitimately to change information held within the file.

56. There are weaknesses in the disaster recovery arrangements for some departments. For example, where back-up tapes are held, they are not routinely encrypted (i.e. this also creates the possibility of illegitimate downloading of data).

57. Inevitably, data security practices vary between departments. They may also vary within departments where individual parts of the department have a measure of autonomy. For example, in the Department of Education Sport and Culture, data security practices vary between schools, for example with regard to the storage of child protective information.[3] The variations in practice between schools are considered in greater detail below.

58. There are also instances where departments have not developed formal data sharing agreements and protocols (i.e. formal processes regarding the circumstances in which information held by a department can be shared with external parties). For example, within the Department for Education, Sport and Culture there was no common practice for the for the sharing of information (including information relating to child protection) with Jersey Police. Steps have been taken to ensure that best practice is understood and is followed consistently.

59. Departments use application software for storing information. In other words, information is held within personal computers using application software such as MS Excel, MS Word and MS Access rather than using the network's resources to store data. Whilst this practice doubtless results from the understandable desire of members of staff to use the most straightforward way of achieving their objectives but the result is that

[2] There are practical constraints which the Department believes limit the risk of abuse of this arrangement.

[3] In fact, the Department is an example of good practice within the States. Some time ago, recognising the risks inherent in there being a large number of separate schools, his Department instituted a programme of actions to ensure that all staff are aware of the risks and the steps which they should all take to minimise these risks. Action is taken to refresh awareness of the importance of best practice and to monitor compliance.

Chief Officers will not be able to control the security of the data held as there are no registers of data held in end user developed applications.

Consequences and risks

60. It is evident from these findings that there are significant variations in practice and that they create opportunities for the abuse of data held by the States.

Variations in practice: security processes

Findings

61. There is no network or server vulnerability server scanning. It would be normal practice in most networks to scan the network and servers regularly to ensure that equipment is working satisfactorily, that malfunctions are identified and that odd incidents (e.g. attempts to hack into a system) are noted.

62. Not all departments monitor the secure destruction of documents. For example, departments may make use of third party contractors to destroy documents. It is not clear that all departments monitor the activities of such contractors to ensure that the requirement for secure destruction are followed.

Department of Health and Social Services

Findings

63. Quite apart from the general issues that are listed above, the review has established that there are weaknesses in the physical security of medical records and documents. For example:

(1) Some of the storage cabinets for adult social care records are broken. A 'fob' is required to access the building but the room where the records are stored is not locked as cleaners and others require access.

(2) The main security system (PAC) is accessible to only one user.

(3) The medical records team is running out of secure storage space for records.

(4) Archived human resources files may not always be stored in the secure human resources archive room.

(5) The main Family Nursing and Home Care building is accessed by both staff and members of the public. In areas where confidential information is held there are signs that state that no access is allowed to the public but there are no locks or physical restrictions ensuring that the public may not enter.

(6) There is no guidance on the use of internal mail for the transfer of confidential records.

(7) For clinics, when there are space restrictions, medical records may be left unguarded in corridors.

(8) The main hospital has a head of security whose remit does not extend to other sites. The arrangements for other sites are not clear.

(9) Access to the medical records department is not controlled by the main hospital security system (PAC). The doors have keypad locks and the codes are not changed on a regular basis. There are no alarms or CCTV. There are also ground floor windows but no additional security measures.

(10) Engineers require access to the medical records department as it is next to the facilities department for the hospital.

(11) Access to Peter Crill House, where the department's administration is located, is not restricted.

(12) The rear door to the medical records storage area leads to the out patients department. This door is kept unlocked during the day.

(13) The out patients department has a shredding service which involves collecting documents which are stored in black bags. In other words, sealed shredding bins are not used.

Consequences and risks

64. PWC reviewed the security within the medical records department as a test of the physical security arrangements made by the States to protect sensitive information.

65. These findings suggest that the physical arrangements that have been made would be inadequate to provide reasonable confidence that the records would be secure against opportunism let alone concerted assault.

Department of Education Sport and Culture

Findings

66. The department maintains a separate education network which is supported by a third party supplier. Although there may be good educational reason for the maintenance of a separate network, there can be no reason for that network being subject to different data security arrangements to those which should apply to the States' network generally. As I have already indicated, the Department is an example of good practice within the States and has made strenuous efforts to minimise risks. It is perhaps an indication of the difficulty of ensuring that data security risks are effectively managed that the review noted the following weaknesses in the management of the education network's security:

(1) E-mails are not generally encrypted.

(2) The third party supplier does not perform any internal network or server vulnerability scanning and so would not necessarily become aware of attempts to hack into the network or malfunctions.

(3) All LAN[4] switches use a generic login and common password (i.e. any member of staff knowing the generic log in and common password can gain access to any of the LAN switches). Unless logins and passwords are guarded appropriately and changed regularly, there is a risk of illegitimate access.

(4) Full disc encryption is not used on networking equipment.

(5) The use of USB devices is not controlled or restricted.[5]

[4] Local Area Network.

[5] The use of such devices is particularly valuable to teachers wishing to prepare teaching and other material out of school hours.

Consequences and risks

67. The effect of these findings is that the policies which should apply to the States' system overall are not applied within the education network thus creating the possibility of illegitimate access to the network and abuse of data. This appears to be an example of the risks created by the absence of central executive responsibility for and authority over the States' network.

SECTION FOUR ~ IMPLICATIONS

Risk

68. The nature and extent of the variations in practice uncovered by the review suggests that the States have not been and are not following best practice in safeguarding the security of data held both within the States network and within departments.

69. One consequence of this is that there must be a significant risk that, sooner or later, the States will suffer the sort of data security failure that has occurred on the mainland.

Organisation

70. The variations in practice uncovered by the review undoubtedly flow in large part from the organisational arrangements for managing the States' network and safeguarding data security.

71. In effect, responsibility for managing data security is one of the responsibilities of a department's chief officer. Where a department is large enough to support an active data security manager, some appropriate safeguarding steps may have been and indeed, as the review has shown, have been taken. However, even where major departments have the resources to support some data security arrangements, practice and effectiveness will vary.

72. This is amply demonstrated by the comments made above in respect of data security within the Departments for Health and Social Security and Department of Education Sport and Culture.

73. Moreover, where a department is not sufficiently large to support an active data security manager, then the arrangements for data security may be patchy.

74. Quite apart from anything else, the fact that data security is a departmental matter means that departmental policies are likely to be regarded more seriously than States-wide policies. Variation from general practice will be tolerated and overall security will be more difficult to secure.

Consistent policies

75. If follows from these comments that it is most unlikely that, under current arrangements, the States:

(1) Will proactively develop a comprehensive set of data security policies, and

(2) Ensure that they are applied consistently and reliably on a States-wide basis

Change and approach

76. On the basis of these comments the following conclusions appear justified:

(1) It is important that the risk of loss or abuse of information held by the States is prevented and, in particular, that proper security policies and practices are implemented throughout the States, without significant variation.

(2) To achieve this the maintenance of data security should be the clear responsibility of an officer with a States-wide remit. Such a person may be the States' Chief Information Officer.

(3) This officer should have responsibility for the following matters in particular

(a) Ensuring that there is a comprehensive map of data held within the States.

(b) Ensuring that there is a comprehensive assessment of the risks to the security of data held by the States which is refreshed on a regular basis.

(c) Ensuring that a comprehensive set of policies is established to manage the risks to the security of data held by the States.

(d) Ensuring that departmental compliance with these policies is monitored on a regular basis.

(e) Ensuring that appropriate corrective action is taken where monitoring demonstrates that unacceptable variations in practice have occurred.

77. There should no tolerance for departments which derogate from States-wide policies. Although circumstances may and indeed will vary between departments, it is important that such variations are not used to excuse variations from the practices required by the

States. It should therefore be incumbent upon Chief Officers to identify cases in which some variation from States-wide policies may be necessary and to agree the appropriate action with whoever becomes responsible for States wide management of data security.

Caution

78. Even if all of these steps are taken, it will not be possible to eliminate all possibility of data security failures. Perfection is not an achievable idea.

79. This should not be an excuse for not taking action. The aim should be to ensure that all reasonable steps are taken to eliminate security failures so that any breaches do not result from the States' inaction and inconsistency.

APPENDIX ONE ~ TERMS OF REFERENCE

Public concern over data security

1 The Island has not been immune to the public concern expressed within the United Kingdom about the public sector's management and protection of data provided to the government sector. Accordingly, it is appropriate to undertake a review of the arrangements in place within the States to protect data.

Terms of reference

2 The review is to be undertaken as a part of the programme of the C&AG:

(1) The review should assess whether the States have established appropriate systems and controls to ensure that public data are held appropriately secure.

(2) This assessment should extend to all parts of the States although attention should be concentrated upon those parts of the States' organisation which in the normal course of business seek and hold information from and about the public.

(3) The assessment should consider whether the standards implemented within central government within the United Kingdom are matched by the systems and controls in place within the States of Jersey.

(4) To the extent that practice within the States does not adopt standards which have been implemented within the United Kingdom, the review should consider to what extent those standards should also be implemented within the States of Jersey.

(5) In this consideration, account should be taken of the risks that poor security practice may lead to actual loss of data, the practicality of implementing such standards, and the cost of implementation.