

Cabinet Office Review of the data incident in the Department for Finance and Personnel

Background

1. Over the weekend of 30-31 May 2009, there was a break-in at the headquarters of the corporate human resources unit of the Department for Finance and Personnel (DFP), Northern Ireland Government, in Royston House in Belfast City Centre.
2. The intruders managed to gain access from an adjacent building and stole 13 laptop computers, primarily by breaking open locked cabinets, though keys to the cabinets were left in an open key safe. A number of the laptops stolen contained a range of sensitive personal and commercial data, including one which contained names, home addresses, payroll numbers, national insurance numbers and dates of birth for all Northern Ireland Civil Service (NICS) employees, and another containing banking information for a subset of NICS employees. Though some files were password protected, encryption was not in place on any of the laptops.
3. Following on from this incident, Cabinet Office were asked by the Northern Ireland government to undertake an independent review in order to identify what lessons might be drawn from the situation within DFP prior to the incident. The full terms of reference for this review were:
 - A review of the Royston House incident, including the storage of personal data on laptops and the methods used to store the laptops;
 - A review of the NICS published procedures for data security as they relate to the Royston House incident and an assessment of how they compare with Whitehall equivalents, including the controls in place governing the transfer of personal data from central databases to mobile electronic storage media;
 - Lessons learned and recommendations, taking account of the high priority of information security, balanced with reasonable business needs.
 - The review is undertaken on the understanding that it forms an element of a broader NICS response to the incident and is not intended for publication.

Approach

4. The review team comprised representatives from Cabinet Office, CESG¹ and the Centre for the Protection of National Infrastructure (CPNI). The review proceeded through an overview of relevant documentation followed by two days of interviews in Belfast at the site of the data incident with the NICS staff involved.
5. The reviewing organisations have no jurisdiction over the DFP and so the contents of this report should be interpreted as advice. The recommendations of the report do not represent mandatory action. This report should also be taken in the context of any other work undertaken to review the impact of this incident or other improvements in policy or guidance.
6. The membership of the review team was selected to provide advice and expertise in the following areas:
 - Physical Security;
 - Network and I.T. Security;
 - Security Policy;
 - Incident Response;
 - Staff awareness and culture;
 - Information Risk Management; and,
 - Data Protection.

Strengths of the response to the incident

7. The evidence available to the review team showed that a number of areas of incident management were positive, and worthy of note.
8. Once the information security breach had been discovered, the review team found that DFP staff were quick to organise themselves and adopt a systematic approach to identifying the data involved in the incident and avoid duplication of effort. DFP also acted promptly and sensibly in deactivating any staff passes that appeared to be missing and deactivating stolen 3G cards, thereby minimising some of the risks that the incident caused.
9. Following the initial incident response, DFP promptly implemented a mechanism to communicate the loss to those affected, both via the FAQ webpage, by email / letter and through the set up of a dedicated help-line. The review team feel that

¹CESG is an arm of GCHQ and the National Technical Authority for Information Assurance

this communication, alongside the prompt action taken to contact banks and the UK payment association APACS, is to be commended.

10. The review team also found that DFP acted promptly and sensibly by ensuring senior officials, ministers and other stakeholders (such as the Information Commissioner's office) were informed. There was also effective consideration and management of the necessary media response. The review team also found that the clear leadership of senior staff throughout the incident was also strong.

Physical Security

11. The review team noted as a possible contributory factor to the incident the move across the NICS, and in DFP in particular, towards open-plan working environments. In the long-term this should encourage improved communal security culture. In the short to medium-term there may be a need to address the current security culture during the transition between working environments across the NICS.
12. The review team found that, following the incident, a number of positive steps have been taken around the physical security of DFP offices in Royston House following the incident. Improvements have included:
 - the implementation of a pass system and visitor books for the buildings;
 - prominent display of security procedures on office doors; and,
 - removal of the system which clearly identified keys in the key safe to their respective containers.

Laptops

13. The review team found that the majority of laptops (12 out of 13) involved in this incident were physically secured in accordance with the current policy.
14. There was also evidence that a process was in place to ensure that any removal of laptops from the main premises was approved by a member of the local senior leadership team, although it was not clear how compliance with this process was ensured.
15. The review team believes that the password protection policy in place on the laptops involved in the incident was sufficient to defend casual attempts to access the data on the system. However without encryption, the information on

the laptops could potentially have been exploited by any sufficiently competent attack.

General Findings

Physical Security

16. As part of the response to the incident, DFP called in the staff of the Security Advisory Unit (SAU) from the Office of the First Minister and Deputy First Minister (OFMDFM), Northern Ireland government, to undertake a full review of the security issues around the break-in. The review team fully endorse the findings and recommendations of that report. There were some issues which fell outside the scope of the SAU report which the review team found to be relevant to the incident.
17. Specifically, the evidence obtained during the review suggested that there was ambiguity over the responsibility for the physical security of the building. This issue was further compounded by the multi-occupancy nature of Royston House, resulting in a lack of clarity over the boundaries of responsibility for various parts of the premises. Whilst the premises officer is currently responsible for these issues in theory, it is a part-time role, and is only partly focused on security issues. The review team did not see sufficient evidence of an effective compliance and reporting regime to ensure adherence to NICS security policy.

Recommendation 1: Clearly allocate the responsibility and accountability for the security of all NICS office space, and ensure that the responsible person is resourced, trained, competent, and supported by senior staff.

18. The review team would recommend building upon the good practice in staff behaviour on leaving the office by ensuring that all offices use a check list to be reviewed by the 'last man out' and an associated sign off sheet to ensure this is being followed. Further more we would encourage the implementation of an independent checking regime of compliance with both the security process itself and the check out process that supports it.

Recommendation 2: Build on this good practice by formalising the policy for the last person leaving the office so that it applies to all NICS office space. Based on and assessment of risk to information and other assets, consider implementing a standard sign out and security checking process for the last person out of the office.

Review the process for ensuring compliance with such policy to ensure this is fit for purpose.

19. The offices in Royston House are some of the first within Northern Ireland to have gone through the Workplace 2010 programme designed to modernise the accommodation of the NICS. One of the areas of focus of this programme is to reduce the number and size of lockable storage units in offices. Whilst reviewing the storage available in Royston House the review team found that much of the lockable storage was not sufficiently robust to meet CPNI guidance.

Recommendation 3: In future, procurement of lockable storage should draw upon the expertise of the Security Advisory Unit in Northern Ireland in order to ensure sufficient physical security. The Security Advisory Unit also have a valuable role to play in providing guidance in selecting and planning for new NICS office space.

Asset management

20. Whilst we support the work undertaken following the incident to identify the assets that had been lost during the incident, the review team found that a register of physical assets held in the office was not in place. Equally, we were not aware of any current information asset register, to take similar consideration of the risk and value of the information held on removable media, or in the office more generally.

Recommendation 4: In line with the measures set out in the Data Handling Review², ensure that information risk is properly represented in departmental risk registers, produce physical and information asset registers and make clear the protection or other action that should be in place for assets of different value.

21. The review team also found that, though there was an alarm system for the DFP office that was broken in to, the system was not turned on and there was little or no effective testing of the alarm system and the subsequent response process. Without this testing programme the alarm system cannot be clearly identified as fit for purpose. Staff who may be responsible for activating alarm systems upon leaving the office need to have a clear understanding of what is

² The data handling review can be found at: http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf and <http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/dhr080625.pdf>

expected of them. Consideration should be given to integrating CCTV into the existing alarm system

Recommendation 5: Develop and implement a regular and effective testing regime for both the alarm system and response mechanism.

22. The review team noted the operation of a visitor pass system at the Royton house site. However there remained some concerns about the overall effectiveness of the physical security. It is still possible to enter the building without proving your need to be there, with little significant challenge at the entrance. It was also possible for visitors to enter or leave the offices without signing out or returning their pass. The review team also found ambiguity in the extent to which staff at the building entrance were performing a security function.

Recommendation 6: Review the access control system for staff entering buildings to ensure it is fit for purpose. This should include a review of the role of the 'guard' position at the main entrance and the arrangements for staff entering offices used by NICS.

23. The review team also found that currently staff are inducted into their local office, but receive little information with regard to the security and wider issues relating to the building itself.

Recommendation 7: Consideration should be given to implementing local building inductions for all staff, including security issues.

Incident Response

24. The review team found that, in a broadly effective response, there did appear to initially be some confusion as to who had overall responsibility for leading and coordinating the response. It was clear to the review team that there was no pre-existing protocol for handling incidents of this kind.

Recommendation 8: Planning should be put in place for the management of any future incidents. This should include a means for clearly identifying who leads the management of an incident, the key personnel involved, and the key actions and

issues that should be considered in responding. Existing Whitehall best practice may be helpful in this respect³.

25. The review team found that the action taken in response to the incident related primarily to the risk of financial fraud. The review team did not find evidence that other risks had been thoroughly considered either in terms of impact or mitigation. In addition, there remain a significant number of individuals whose personal information was lost that have not yet been contacted.

Recommendation 9: A systematic assessment of the potential impact of this loss should be made and appropriate mitigation put in place. Action to address the risks to those not yet contacted about the loss should also be taken.

Removable media

26. The review team found that there was no encryption in place on the laptops involved in the incident, though there was a NICS wide policy of encryption of removable media containing personal data. At the time of the incident this policy applied to sensitive personal data only. The review team found that there was some confusion as to the process and accountability for identifying removable media that required encryption. There was also no evidence of action to ensure compliance with encryption policy. The review team did see evidence of encryption in use for USB memory sticks.

Recommendation 10: The process and accountability for identifying removable media that require encryption should be made clear. This should include measures to ensure compliance with this policy.

Recommendation 11: In the interests of greater protection for all personal data, and greater clarity in identifying the information assets that this policy should apply to, consideration should be given to implementing a programme for the encryption of *all* removable media containing personal data.

27. The review team found that the processes for issuing and returning laptops were not clear, and that the security guidance issued to staff could be improved.

³ The Cabinet Office guidance on Incident management will be made available to DFP and NICS more broadly

Recommendation 12: In line with the measures set out in the Data Handling Report and Data Protection legislation, processes for issuing and returning laptops should be reviewed to ensure they are fit for purpose and made clear to all staff with access to laptops. Guidance to staff on the secure use and protection of laptops should be reviewed and made clearer. This should include the effective use of Kensington locks in physically securing laptops.

Data management

28. The review team found that the personal data involved in the incident had been placed on laptops for legitimate and ongoing business purposes. However there was no evidence of consideration of alternative options for managing, transferring and minimising this data. Furthermore the review team found no clear accountability for the security and protection of the data concerned, and no evidence that risk assessment or protective marking had been applied to the data.

Recommendation 13: In line with measures set out in the Data Handling Report, the accountability for the security and proper handling of personal data should be made clear. This should encompass both existing senior roles such as the Senior Information Risk Owner and also those accountable for and knowledgeable about specific data sets to ensure compliance with policy and to provide the SIRO and accounting officer with assurance about the personal information held and managed. Clear policy should be developed for the means of transferring personal information. The measures set out in the Data Handling Review may be helpful in this respect⁴.

Recommendation 14: Personal data held and transferred should be reduced to only those necessary to meet business need. Such data should only be held for as long as necessary to meet business need. Data no longer required should be disposed of securely.

Policy and Guidance

29. The data review team found that existing guidance and policy on information security has built up iteratively over time and staff were often not clear as to what actions they needed to take.

⁴ The Data Handling Report (paragraphs 13-15 pages 3-4) provides information on different options for transferring information

http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf

Recommendation 15: Existing information security policy and guidance should be reviewed with a view to producing a clear and succinct statement of mandatory policy, and to provide a single authoritative source of guidance.

Culture

30. The data review team heard several reports relating to the significant workloads of the staff using the data involved in this incident. In common with a number of other data losses there was a clear focus on 'getting the job done' at the expense of other considerations. The review team found that this may have been a contributory factor in the incident. Whilst improvements have been made since the incident, the review team found that there was further scope to improve the security advisory and culture.

Recommendation 16: Action should be taken to address the organisational culture with regard to the handling of information. This might include raising awareness, training⁵ for all staff handling data, and a clear statement of the HR and disciplinary position for data losses. Furthermore consideration should be given to using the new CPNI security awareness culture tool to help establish the desired security culture and identify any gaps

The Central Sponsor for Information Assurance – Cabinet Office
23rd July 2009

⁵ For example the Cabinet Office's protecting information e-learning, which will be made available to DFP and NICS more broadly