Privacy Commissioner
Te Mana Matapono Matatapu

PORTABLE STORAGE DEVICE SURVEY

May 2010

New Zealand Public Sector

P/0198 /A223526

Contents

1. INTRODUCTION

In 2009 we surveyed 42 government agencies about their controls on the use of portable storage devices (PSDs). Following publication of the survey results we signalled that a follow up survey would be undertaken to find out whether government agencies had responded to the feedback we gave them and taken steps to better protect New Zealanders' personal information. This 2010 survey report delivers on that undertaking.

PSDs are small, lightweight, portable, easy to use devices capable of storing and transferring large volumes of data. They include USB sticks, cellphones, iPods, PDAs (personal digital assistants), iPhones and netbooks.

The use of PSDs in the workplace potentially presents major security risks, particularly if the devices contain unsecured sensitive data. They can be easily lost, misplaced or stolen. The storage capacity of PSDs has grown dramatically in only a few years, exposing organisations to risks of major data breaches. As several high-profile incidents overseas illustrate, these data breaches can seriously damage both the reputation of the agency concerned and the trust that the public has in that agency.

The results show that while many government agencies have generally improved security on PSDs there are some key agencies that continue to have inadequate controls.

Some of the key findings are:

- 29 of the 42 agencies that responded to this year's survey prohibited the use of personal PSDs for work purposes (14 of 37 agencies last year);
- an estimated 120 organisation owned PSDs have been lost or stolen in the 12 months to March;
- 79 percent of agencies surveyed keep a PSD register (62 percent last year);
- 76 percent or agencies surveyed used hardware or software controls (59 percent last year);
- many agencies have controls only on some PSDs they provide to staff; and

- agencies which primarily hold sensitive or classified information continue to out - perform agencies which primarily hold personal information.

Last year we said we wanted agencies to get it right before they get it wrong. Many government agencies have made a promising start but more needs to be done to protect New Zealanders' personal information.

Marie Shroff
Privacy Commissioner

2. METHODOLOGY

This second New Zealand survey follows the format used in the Australian Privacy Commissioner's survey released in April 2009[1]. Although the format has been modified since last year, many of the questions are the same as last year to allow us to compare results. We selected 42 state sector organisations for participation in the survey:

- 35 Public Service Departments;
- 6 Non-Public Service Departments; and
- 1 Crown Entity.

On 19 February 2010 we sent covering letters with an enclosed survey to each Chief Executive (or equivalent) explaining the purpose of the survey. At the same time, we sent an electronic version of the survey to each CE's Executive Assistant, requesting that they forward the survey to the staff member nominated by the Chief Executive to complete it.

The survey consisted of 45 questions. These fitted into the following categories:

- use of hardware or software controls;
- use of organisation-owned PSDs; and
- use of privately-owned PSDs

All 42 agencies surveyed responded in time to be included in the report.

The survey results are presented in four parts as follows;

- combined results of all 42 agencies on the use of hardware or software controls;
- combined results of all 42 agencies which allow use of organisation-owned PSDs;
- combined results of the 13 agencies which allow use of privately owned PSDs; and
- a comparison of key results after agencies were separated into three groups:

Group 1	Agencies that hold large amounts of personal information
Group 2	Agencies that primarily hold classified or sensitive information
Group 3	Agencies that hold relatively small amounts of personal information

[1] See Portable Storage Devices and Australian Government Agencies Personal Information Survey at http://www.privacy.gov.au/materials/types/download/9292/6866

3. SUMMARY OF RESULTS

The survey results show that progress has been made by many government agencies since our last survey 12 months ago. However there are still some key agencies that are below par and need to increase their efforts to secure information in their care.

On the positive side, there has been an increase in the number of agencies which have controls on the use of PSDs through new policy and/or hardware and software controls.

Limits on the use of PSDs

Hardware and/or software controls are being used by more agencies to control PSD use (32 of 42) compared to last year (22 of 37). Agencies which primarily hold sensitive or classified information continue to out-perform the two other agency groups. All Group 2 agencies (see Appendix A) use hardware and/or software controls and keep a register of organisation owned devices.

While there has been an increase in the number of agencies which use policy to control the use of PSDs, we believe that the quality and delivery of PSD policy could be improved. Twenty nine agencies responded that they have a policy on the loss or theft of PSDs; however, only 21 have a policy on the disposal of PSDs; while 16 agencies have a policy on when data should be deleted from PSDs. Staff are mostly responsible for keeping themselves up to date with policy. Thirty four agencies responded that they made staff aware of policy by providing it on the agency intranet. Auditing to ensure that staff are following policy remains poor (10 out of 38 agencies).

Last year we expressed our concern at the number of agencies which allowed staff to use their own PSDs for work purposes. It is pleasing to see that two-thirds (29 or 42) of agencies now prohibit the use of personal PSDs for work purposes (last year 14 of 37).
Results show that controls are weaker on privately owned PSDs used for work purposes. None of the agencies record private PSDs on a PSD register while 11 of those 13 agencies cannot track transfers to those PSDs.

Requirements for how PSDs are used

Thirty three of the 42 agencies surveyed said they have a register of PSDs. Two thirds (22) of agencies which have a PSD register perform an annual stock-take of devices to verify that each device is still in use and held by the staff member. However, most agencies only keep a record of specific devices. Laptops and smart phones are more commonly on the register, while USB sticks are included in less than half of all registers.

The tracking of file transfers to PSDs remains poor with 30 of the 42 agencies surveyed having no technical ability to do so. Five agencies responded that they have the ability but choose not to track transfers.

Twenty five of the 42 agencies surveyed said that they have experienced the loss or theft of organisation owned PSDs in the last 12 months. The survey reveals that 120 organisation owned PSDs were lost or stolen in the last 12 months.

Our survey did not conclusively determine whether there has been an increase in the use of encryption on PSDs since last year. However, 37 of 42 agencies responded that they provide encryption on all PSDs (5 agencies) or on specific devices (32 agencies).

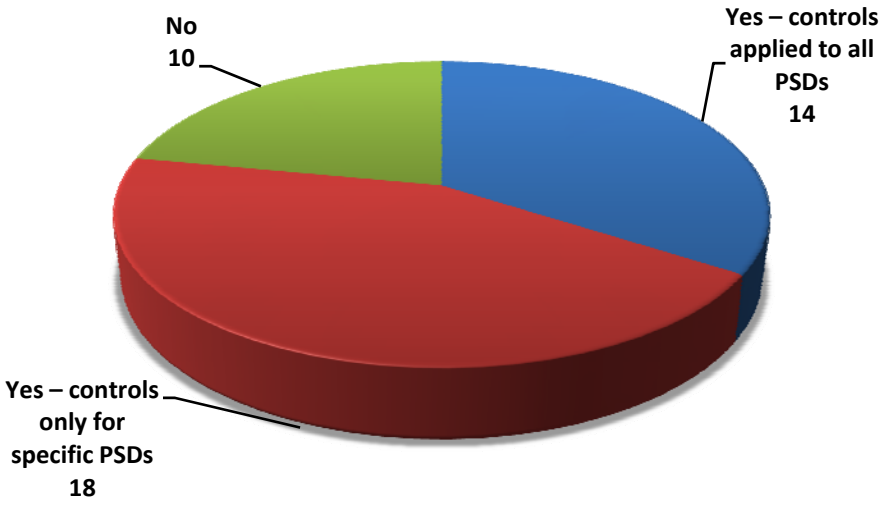
4. RECOMMENDATIONS

Based on the results of both surveys, we continue to recommend that:

- agencies have a formal policy on PSD use that is actively and effectively communicated to staff;
- staff should be made aware of the need to report the loss or theft of a PSD, and know the procedures for doing so;
- it should be clearly explained to users how and when to delete data from PSDs;
- encryption should be used for all PSDs that are likely to store personal information;
- strict limits on the use of personal PSDs should be enforced, in combination with providing suitable corporately-owned PSDs; and
- agencies that hold large amounts of personal information should not rely solely on policy but also use hardware and/ or software controls to restrict or control the use of all PSDs.

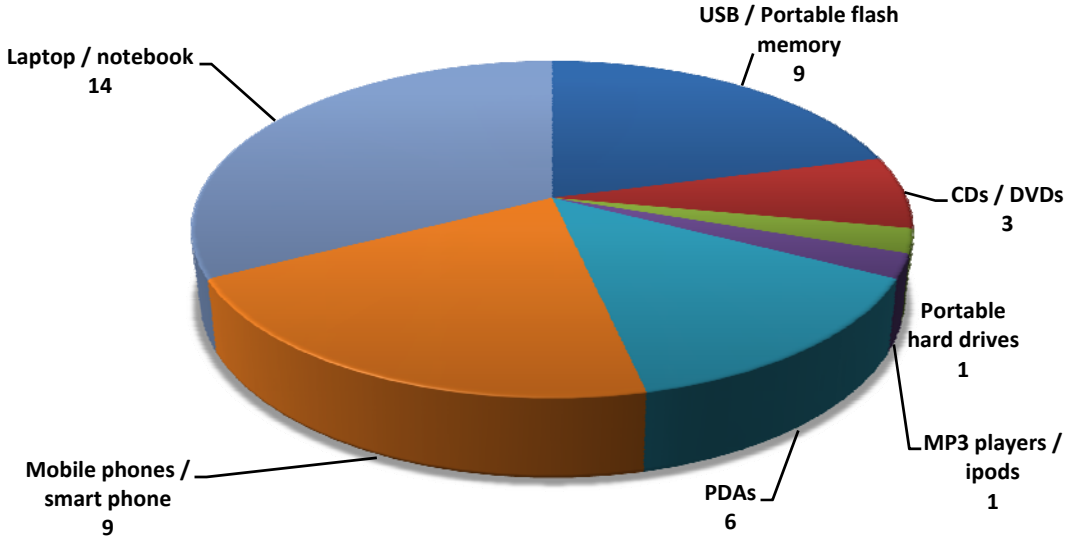
5. RESULTS: USE OF HARDWARE OR SOFTWARE CONTROLS

5.1 Does your organisation use hardware or software controls to restrict or control the use of PSDs?



Three quarters of agencies have controls on all or selected PSDs (2009 – 59%)

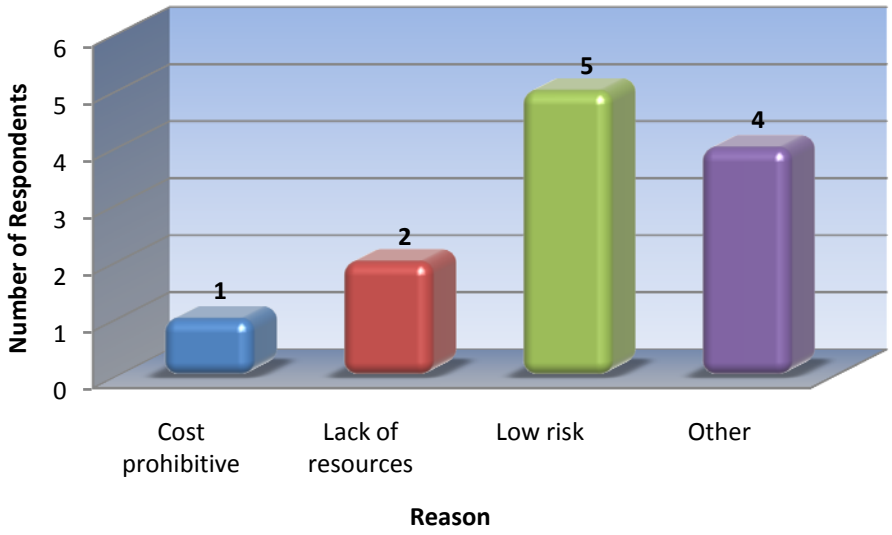
Of the 18 agencies which only apply controls to specific PSDs, the following chart shows which PSDs those controls apply to.



5.2 Does your organisation intend to implement hardware or software controls in the next 12 months (where no controls exist)?

Of the 18 agencies which have limited controls, 12 intended to implement further controls. Of the 10 agencies which have no controls, four intend to implement controls.

5.3 What is the main reason your organisation does not intend to implement either hardware or software controls in the next 12 months?



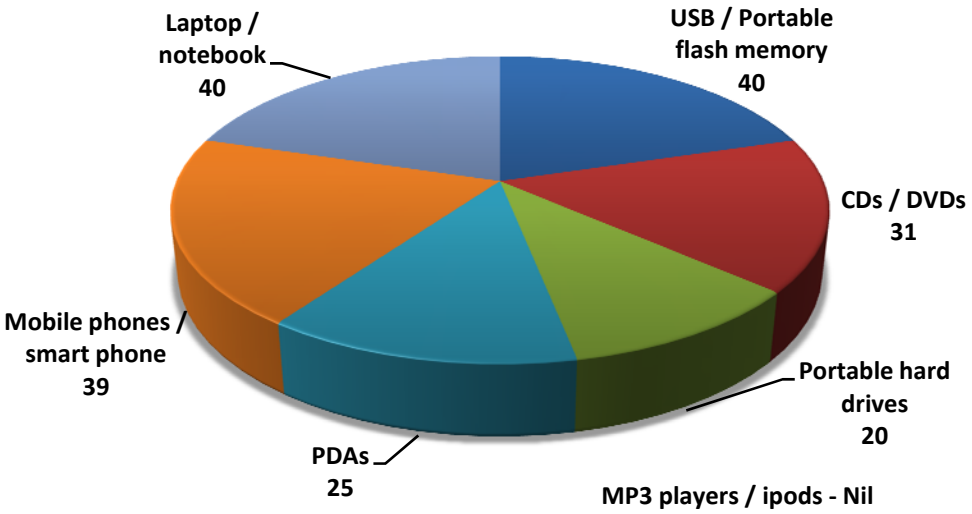
Of those that responded 'other' to this question, some agencies advised that a combination of cost, risk, and lack of resources were applicable. Other reasons included the reliance on policy controls and a likely negative reaction to controls by members of the organisation.

6. RESULTS: USE OF ORGANISATION-OWNED PSDS

6.1 Does your organisation provide PSDs to any staff or contractors?

All the agencies surveyed provided PSDs to either staff only (23) or staff and contractors (19).

6.2 What types of PSD does your organisation provide?



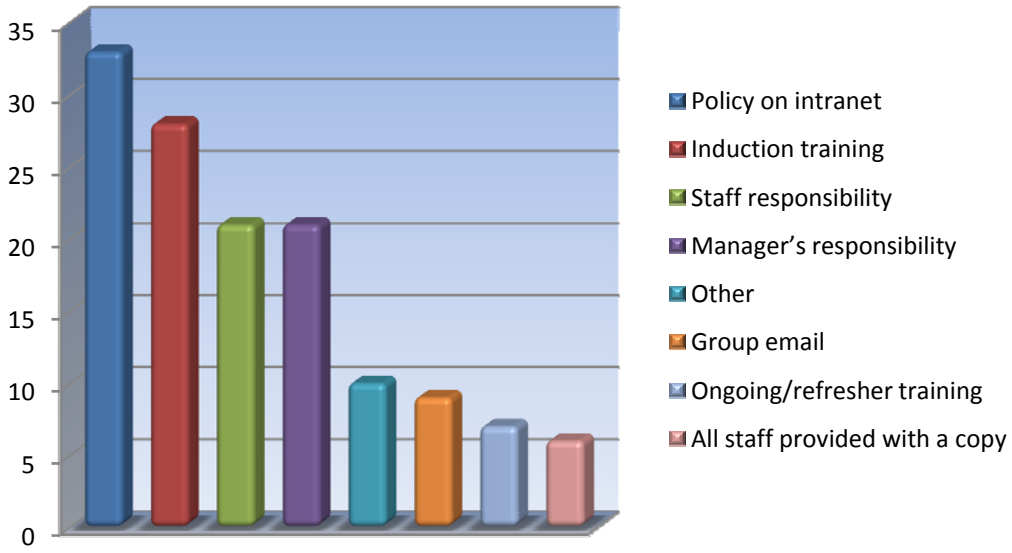
6.3 Does your organisation use documented policy to restrict or control the use of organisation owned PSDs?

Ninety percent of agencies surveyed (38 out of 42) responded 'yes' to this question. This is a useful increase over last year's result (28 out of 37).

Of the four agencies which responded 'no' to this question, two intend to develop a policy in the next 12 months.

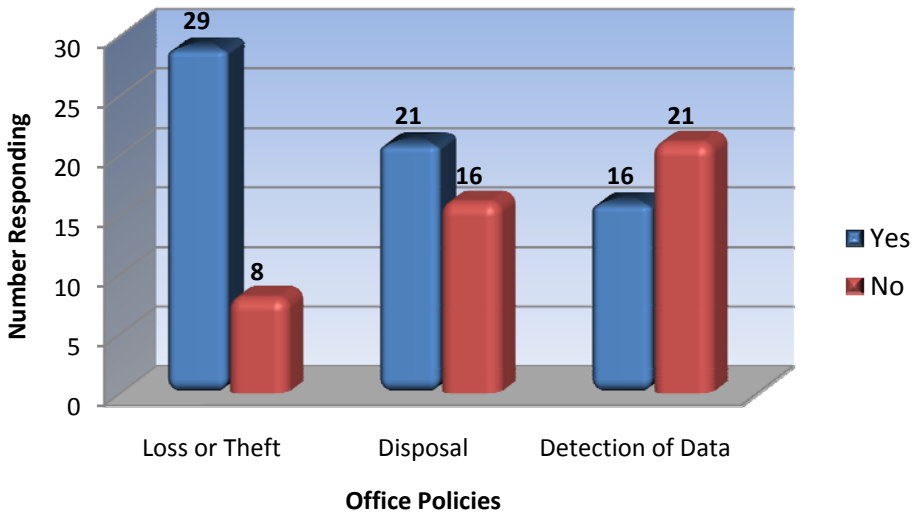
Of the 38 agencies which have a policy to restrict or control the use of PSDs, 31 agencies have a policy covering all PSDs, while seven agencies have policy on specific devices only.

6.4 How do you ensure that staff are made aware of the policy?



6.5 To get an indication of the quality of the policy held by agencies on the control and use of PSDs we asked the following three questions:

- Does the policy describe procedures for reporting loss or theft of a PSD belonging to your organisation?
- Does the policy describe procedures for disposing of PSDs that are no longer required?
- Does the policy describe when personal information should be deleted from PSDs?



6.6 Do you perform a scheduled audit to ensure PSD policies/ procedures are followed?

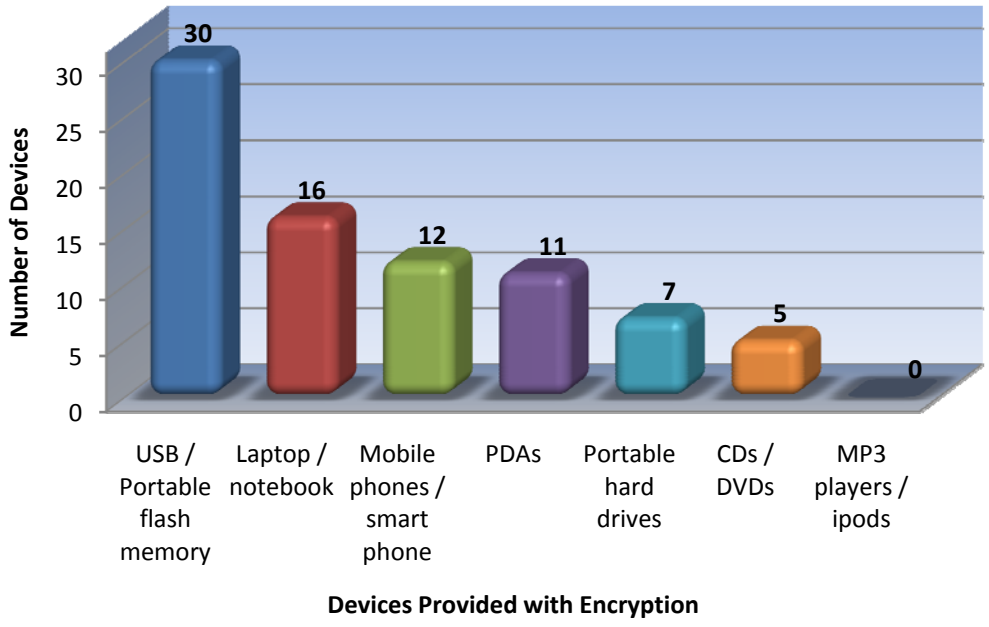
Of the 38 agencies which have policies to restrict or control the use of organisation owned PSDs, only 10 agencies report that they perform a scheduled audit to ensure those policies are adhered to (28 of the 38 or 74% do not perform a scheduled audit).

6.7 What types of PSD are provided with an encryption feature?

Of the 42 agencies surveyed:

- 5 agencies provide an encryption feature on all PSDs;
- 32 agencies provide an encryption feature on specific PSDs; and
- 5 agencies do not provide encryption.

Of those that provide an encryption feature on specific PSDs, the following chart shows that USB devices are generally provided with encryption while other devices are less commonly encrypted.



6.8 Where PSD encryption is provided, is its use mandatory?

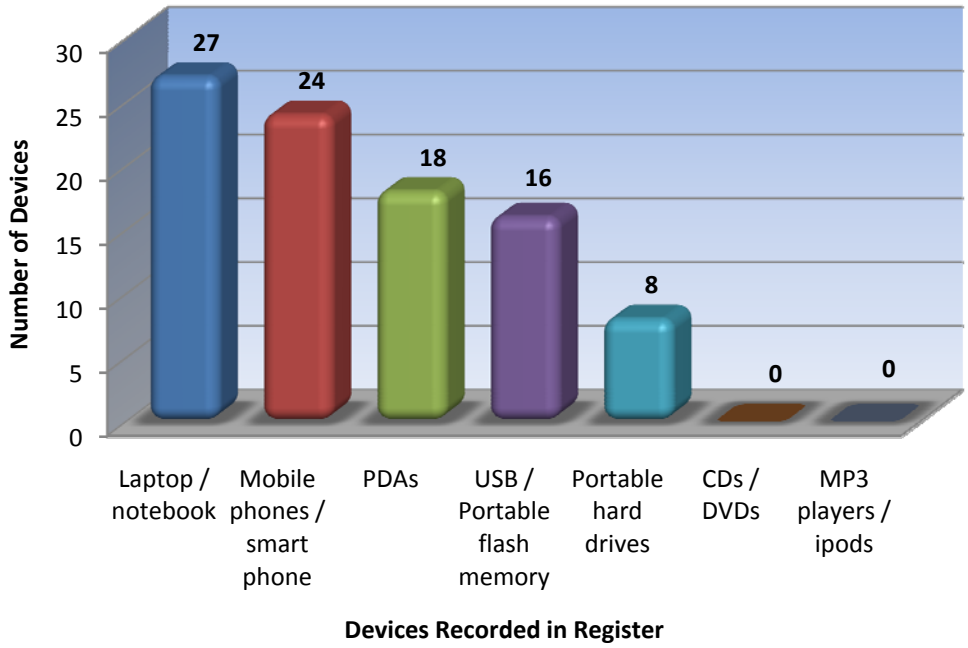
Twenty agencies responded that where encryption was provided, its use was mandatory on all PSDs, while 15 agencies responded that the use of encryption depended on the classification of the information to be stored onto the device. In total, 35 of 37 agencies (95%) require encryption in all or in some situations. The remaining two agencies do not require encryption to be used with PSDs.

6.9 Has advice been sought from the Government Communications Security Bureau (GCSB) on the use of PSD encryption?

Twenty one of 41 agencies responded that they have consulted with GCSB.

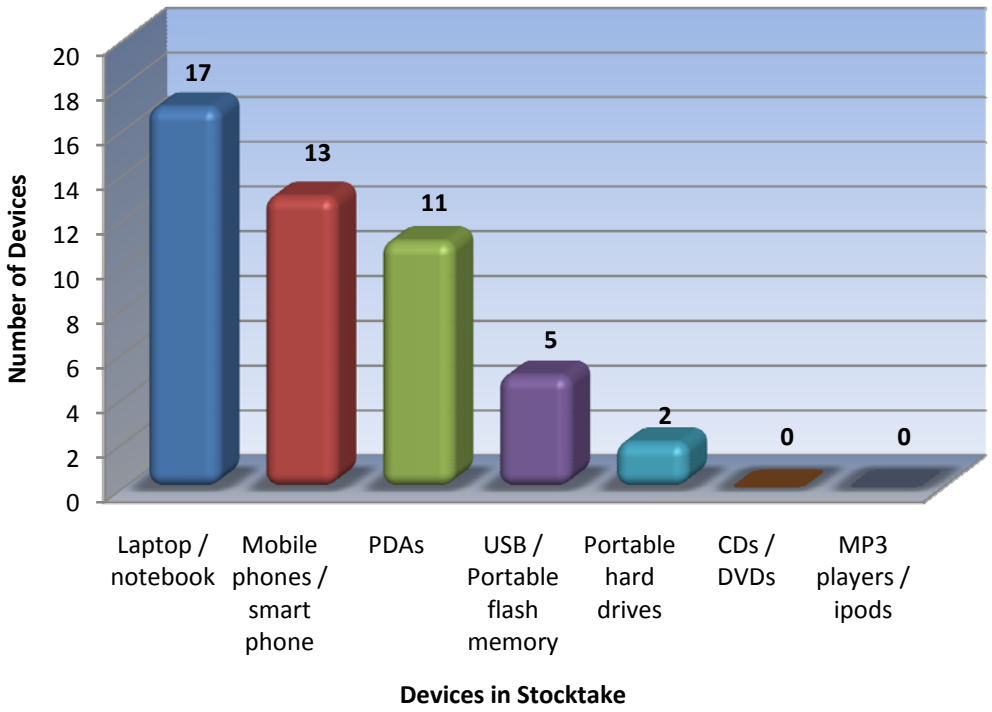
6.10 Does your organisation keep a register of organisation-issued PSDs?

Thirty three of 42 agencies keep a register of PSDs. Five of the 33 agencies keep a register of all PSDs while the remaining 28 keep a register only for specific devices. For the agencies that do not keep a register of all devices, the following chart shows which PSDs are included.



6.11 Does your organisation undertake a stock-take of the PSDs recorded in the register to verify that the device is still in use / held by the staff member / contractor?

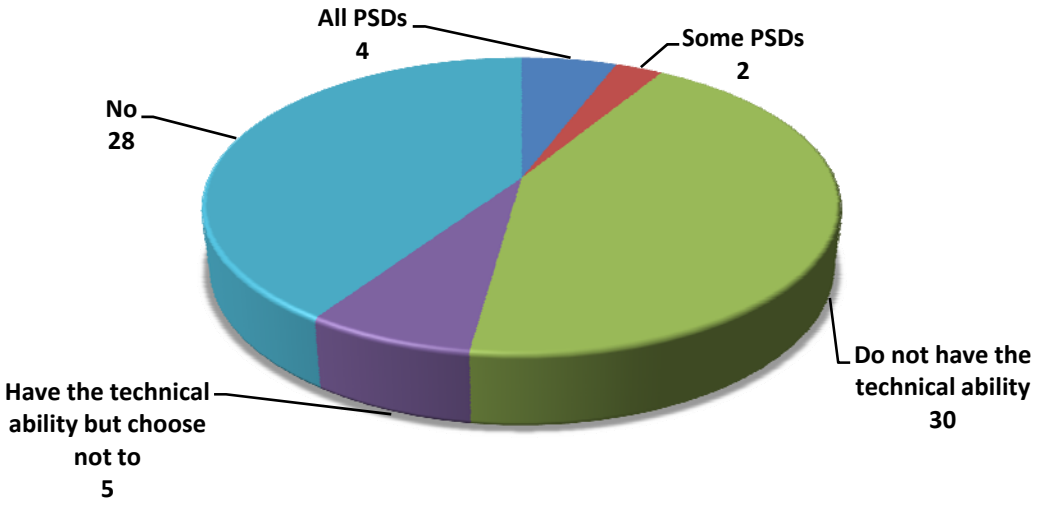
Twenty two of the 33 agencies which have a PSD register perform an annual stock-take of devices. Eleven agencies do not perform a stock-take. Four of the 22 agencies perform a stock-take on all PSDs while 18 agencies only audit specific PSDs. For the agencies which perform an audit on specific PSDs, the following chart shows which devices are included.



6.12 Why does your organisation not undertake a PSD stock-take?

Of the 11 agencies which do not perform a stock-take, four cited low risk as the reason, one that it was a cost prohibitive exercise and six responded with other reasons which included time constraints and complexity.

6.13 Does your organisation track transfers of files or data to organisation-owned PSDs?



6.14 In the last 12 months, has your organisation experienced any loss or theft of organisation-issued PSDs?

Twenty five of the 42 agencies (60%) responded that they have experienced the loss or theft of organisation-owned PSDs in the last 12 months.

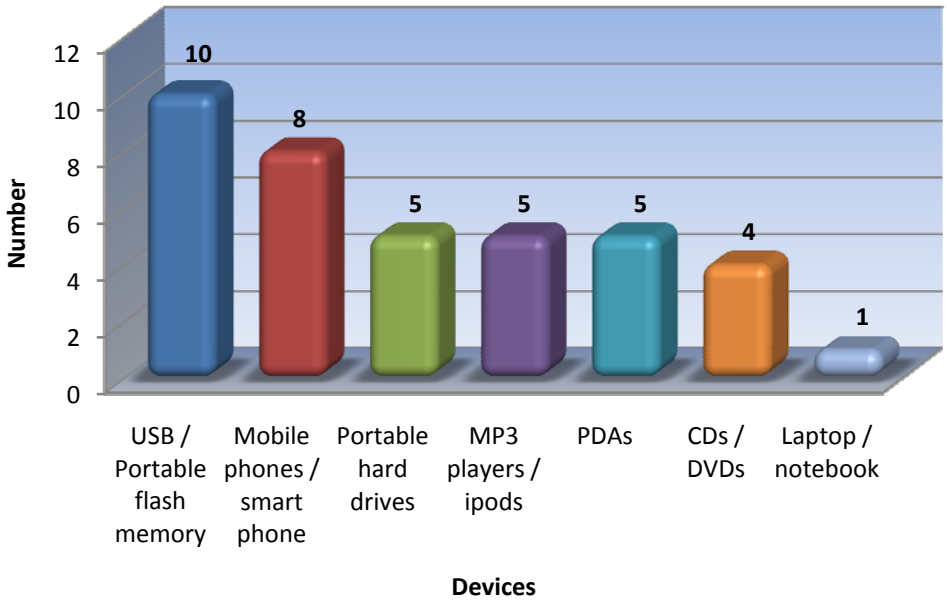
The survey reveals that an estimated 120 organisation-owned PSDs were lost or stolen in the last 12 months.

In almost all occasions, agencies became aware of the loss or theft of a PSD through staff notification.

7. RESULTS: USE OF PRIVATELY-OWNED PSDS

7.1 Are staff allowed to use their own PSDs for work purposes?

Thirteen of the 42 agencies (31%) allow staff to use their own PSDs for work purposes. Of the 13 agencies which allow use of private PSDs, one allows use of any PSDs while 11 only allow use of specific types of PSD (see chart below).



7.2 Does your organisation have any separate policy on the use of private PSDs?

One of the 13 agencies has a separate policy on the use of privately owned PSDs while five others intend to develop a policy during the next 12 months.

Two agencies cited low risk as the reason for not developing a policy and three others mentioned that their policies on PSDs cover both organisation and privately owned devices.

7.3 Does your organisation keep a register of privately owned PSDs used for work purposes?

None of the agencies surveyed keep a register of privately owned PSDs used for work purposes.

7.4 Does your organisation track transfers of files or data to privately-owned PSDs?

Eleven of the 13 agencies do not have the technical ability to track transfers. One agency tracks all transfers while another only tracks specific devices.

7.5 In the last 12 months, has your organisation experienced any loss or theft of personal information stored on a privately-owned PSD?

Two of the 13 agencies said that they had experienced the loss or theft of personal PSDs used for work purposes while 11 responded no to this question.

7.6 Is the use of PSD encryption mandatory on privately-owned devices?

Three agencies responded that they require the use of encryption in certain circumstances while the remaining 10 agencies responded that PSD encryption was not mandatory.

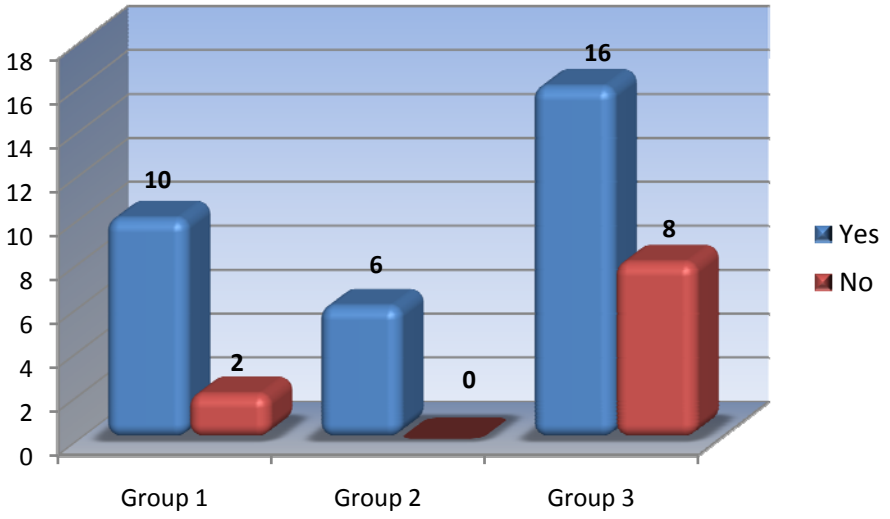
8. KEY RESULTS BY AGENCY GROUP

Group 1 Agencies that hold large amounts of personal information

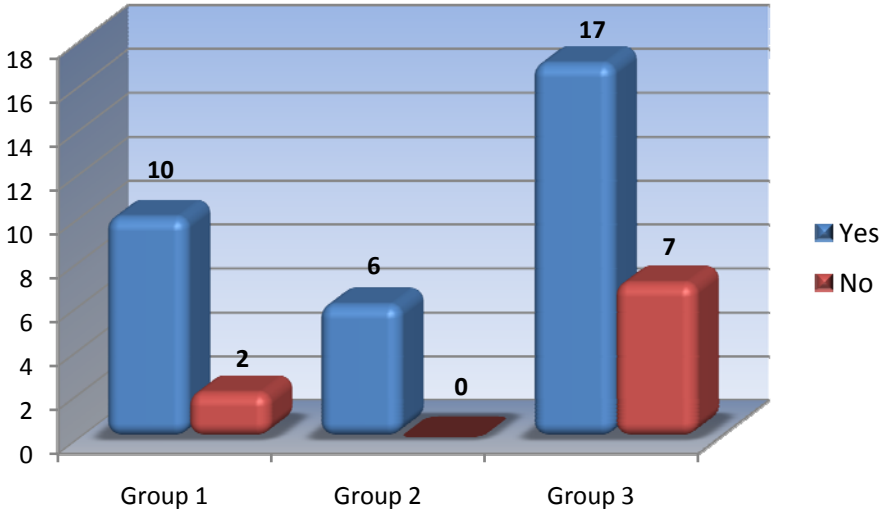
Group 2 Agencies that primarily hold classified or sensitive information

Group 3 Agencies that hold relatively small amounts of personal information

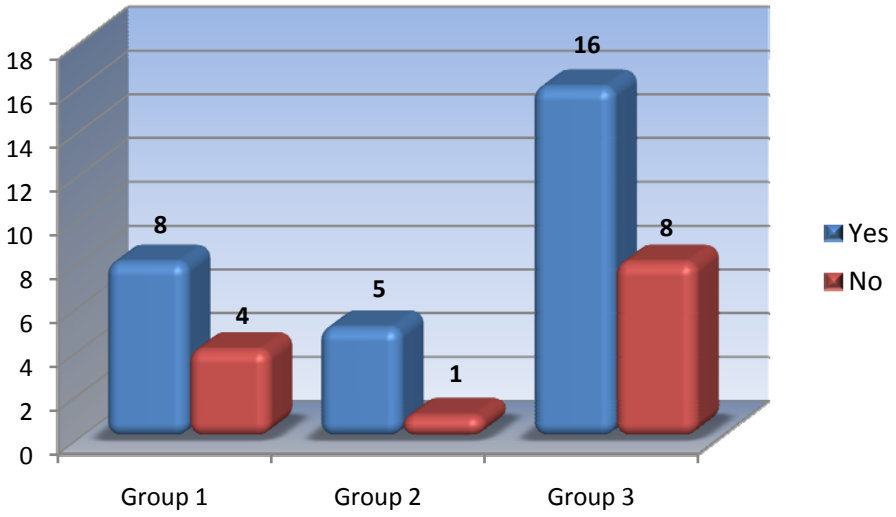
8.1 Does your organisation use hardware or software controls to restrict or control the use of PSDs?



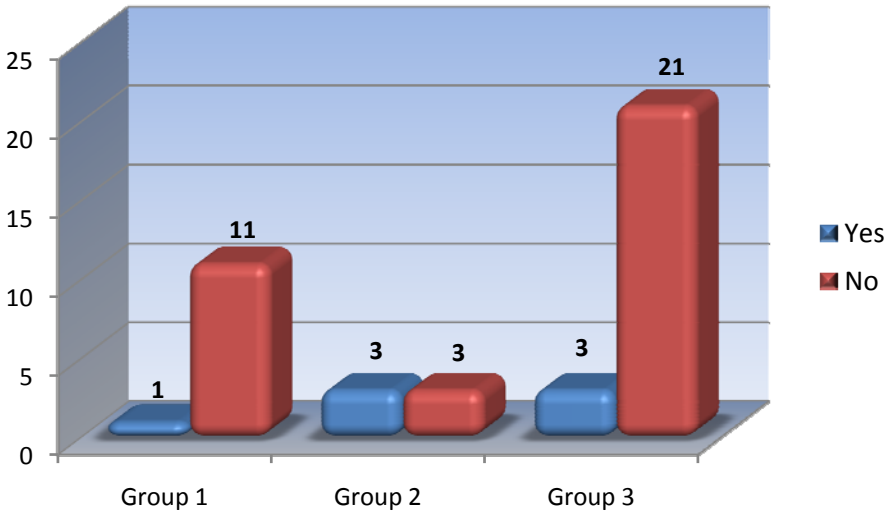
8.2 Does your organisation keep a register of organisation-issued PSDs?



8.3 Are staff prohibited from using their own PSDs for work purposes?



8.4 Does your organisation track transfers of files or data to organisation-owned PSDs?



Appendix A: List of surveyed organisations by group

Group 1

Statistics New Zealand
Department of Corrections
Inland Revenue
New Zealand Police
Accident Compensation Corporation
Department of Labour
NZ Customs Service
Ministry of Justice
Ministry of Social Development
Department of Internal Affairs
Ministry of Education
Ministry of Health

Group 2

New Zealand Security Intelligence Service
Department of the Prime Minister and Cabinet
New Zealand Defence Force
Serious Fraud Office
Ministry of Foreign Affairs & Trade
Government Communications Security Bureau

Group 3

Ministry of Pacific Island Affairs
Ministry of Fisheries
New Zealand Food Safety Authority
Department of Conservation
Ministry for Culture and Heritage
State Services Commission
Crown Law Office
The Treasury
Ministry of Agriculture and Forestry
Parliamentary Counsel Office
Te Puni Kokiri
Ministry of Research Science and Technology
Ministry for the Environment
Land Information New Zealand
National Library of New Zealand
Ministry of Defence
Department of Building and Housing
Ministry of Economic Development
Education Review Office
Ministry of Women's Affairs
Parliamentary Service
Archive New Zealand
Office of the Clerk of the House of Representatives
Ministry of Transport