Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Stolen Laptop

Department(s) Compiling the Report

ST

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
19-Dec-09	19-Dec-09		23-Dec-09

Summary description of the incident

A laptop was stolen from the home of an ST staff member.

Summary of cause

Support laptops are supplied to facilitate out-of-hours access for the provision of system support from home.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☐
- Financial ☑
- Legal ☐
- Reputational ☐

Description

Residual value of leased laptop - estimated less than $3000

Severity of actual impact

Insignificant

Summary action plan

No new action items arising.

Estimated Completion Date

N/A

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

Please submit Incident Report to RM Operational Risk

STOLEN LAPTOP

1. EXECUTIVE SUMMARY

On 19th December a laptop was stolen from the home of an ST staff member. The total financial cost was around $3000. There is no risk of unauthorised access to sensitive data arising from this theft.

2. SEQUENCE OF EVENTS

Late on Friday 18th or early on Saturday 19th December an RBA laptop barcode BRS0910081 was stolen from the home of while he slept. had been using the laptop until 10:30pm, completing work via the VPN. The theft was part of a general home burglary which was discovered at 8:00am. Police were called and an event number was allocated.

3. SYMPTOMS

The lost laptop was identified as part of the post home-burglary inventory.

4. IMPACT

The laptop is used for on-call support. It had standard software for accessing the VPN but is useless for this purpose without associated authenticating material (i.e. logon, password, VPN token). No logons or passwords were stored on the laptops. There was no sensitive information stored on the laptop.

The Bank carries the financial risk on all such thefts. In general this equates to the pro-rata value of the lease plus some residual. ST has not yet received advice from the leasing company but it is estimated the Bank will be liable for around $3000 in total.

5. CAUSE

Support laptops are supplied to facilitate out-of-hours access for the provision of system support from home.

is living in short-term rental accommodation while between buying and selling houses and this is the second theft from the property during his tenure. We will discuss with him any options for reducing risk of further losses within the constraints of his current arrangements.

6. ISSUES

Issues that have been highlighted by this incident include:

- Risk (not realised in this incident) of unauthorised access to data on equipment removed from Bank premises.

7. RISKS AND REFERENCES TO BUSINESS IMPACT ASSESSMENT

This incident relates to the following risks in the ST Risk Register. There are no changes to the risks as a result of the incident:

- Risk 02 Op/Physical Security/Safeguarding Assets – Theft due to inadequate security.
- Risk 24 Op/External/Third Party – Theft of sensitive information by media or third party.

The incident does not relate to a process in the ST Business Impact Assessment.

8. RECOMMENDATIONS

In this case, there was no sensitive data stored on the laptop but this may not always be the case in future thefts. Recommendations to reduce the risk of unauthorised access to sensitive data were made in an incident report of 26 November 2009 entitled STOLEN LAPTOPS. No further recommendations are made as a result of this incident.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
No new actions arise from this incident.				

10. DISTRIBUTION LIST

Name	Name	Name

11. SIGN OFF

Title	Name	Signature
ST Department Head		

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Stolen laptop - 3 January 2010

Department(s) Compiling the Report

Payments Settlements

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
03-Jan-10	03-Jan-10	04-Jan-10	15-Jan-10

Summary description of the incident

An RBA laptop has been stolen from the home of a PS staff member.

Summary of cause

Laptops supplied to PS senior management for on-call and management support functions are normally stored at the home of the staff member.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☐
- Financial ☑
- Legal ☐
- Reputational ☐

Description

Residual value of leased laptop.

Severity of actual impact

Insignificant

Summary action plan

Issue guidelines to PS management for external storage of Bank information. These include use of laptop hard drive password protection and RBA-issued encrypted USB memory sticks.

Estimated Completion Date

01/02/2010

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☐
- Yes ☑ ▶ Please select
  - Controls ☑
  - Risk Ratings ☐
  - Risk Description ☑
  - New Risk ☐

Please submit Incident Report to RM Operational Risk

STOLEN LAPTOP – 3 JANUARY 2010

1. EXECUTIVE SUMMARY

A laptop was stolen from the home of a PS staff member. The laptop was acquired in November 2008; the estimated cost payable to the leasing company is about $1500. There is no risk of unauthorised access to sensitive data arising from this theft.

2. SEQUENCE OF EVENTS

On Sunday 3 January 2010 an RBA laptop barcode RBA2008475 was stolen from the home of . The theft was part of a general home burglary. Police were called and an event number was allocated.

3. SYMPTOMS

The lost laptop was identified as part of the post-burglary inventory.

4. IMPACT

The laptop was made available as part of PS arrangements for management to meet on-call and other requirements to support PS operational functions. It is possible, although unlikely, that some recent PS working documents were stored on the computer. Any such documents would not contain material of a sensitive nature.

The laptop had standard software for accessing the VPN but is useless for this purpose without associated authenticating material (i.e. logon, password, VPN token). No logons or passwords were stored on the laptops and the VPN token was not stolen.

The Bank carries the financial risk on all such thefts. In general this equates to the pro-rata value of the lease plus some residual. ST has not yet received advice from the leasing company, but it is estimated that the Bank will be liable for around $1500 in total.

5. CAUSE

Laptops supplied for out-of-hours work are usually kept at the home of the staff member involved.

6. ISSUES

The main issue highlighted by this incident is the risk (not realised in this incident) of unauthorised access to data and information on equipment removed from Bank premises. This includes laptops and portable memory sticks.

7. RISKS REGISTER ASSESSMENT

This incident relates to the following risks in the PS Risk Register:

- Risk L05 Op/Information Technology/System Access – Theft of data or other access to confidential data by unauthorised persons. Additional controls will be added to this risk.

- The risk grouping Op/Physical Security/Safeguarding Assets is also relevant. However these risks relate to Bank equipment on Bank premises. In this case, the laptop was stored at the home of a staff member. The register will be amended to reflect loss of Bank equipment stored off-site.

Incident Action Items	Corresponding Risk Register Item	Changes to Risk Register
Action item 1	n.a.	
Action item 2	L05	Additional controls to be added.

8. RECOMMENDATIONS

In this case, no sensitive data is known to have been stored on the laptop but this may not always be the case in future thefts. PS has been advised that the RMC was provided with an update on the use of hard drive encryption and ST undertook to complete documentation and procedures suitable for distribution to staff.

Specific steps for data and other Bank information on PS laptops, external hard drives and portable memory are noted in the action items below.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
1. Review arrangements for electronic storage of RBA information offsite.	Low	High	Completed	Head of PS
2. Issue guidelines to PS management for external storage of Bank information. Specific action items in this include: (a) Staff with Bank laptops to password protect the hard-drive. Interim procedures to be provided. (b) In general, no information to be stored externally unless on an RBA laptop (password protected hard drive) or on an RBA issued encrypted USB drive ( ) (c) will replace earlier RBA issued sticks with RITS documentation. (d) All data currently stored that does not comply with guidelines to be deleted. (e) VPN tokens not be kept with laptops off-site	Low	Med	8/01/2010 Completed. Procedures emailed to PS staff 13/01/2010. ordered from ST 8/01/2010.	Head of PS

10. DISTRIBUTION LIST

Name	Name	Name

ADDENDUM

Incident Report – Stolen Laptop – 3 January 2010

Reference to Business Impact Assessment

This incident does not relate to any key processes identified in PS Business Impact Analysis.

There are no changes to the Business Impact Analysis as a result of the incident.

Payments Settlements Department
15 January 2010

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Handling of confidential information

Department(s) Compiling the Report

Financial Administration

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
12-Jan-10	05-Mar-10	19-Mar-10	19-Mar-10

Summary description of the incident

During Financial Administration's (FA's) BRS test on 12 January, Accounting, Analysis & Policy (AAP) staff left a document containing personal staff details on a desk in the pod this document should have been destroyed after the test on the same day. The document was found by Audit Department on 5 March when they were undertaking tests at the BRS. After alerting the Senior Manager AAP, the document was destroyed.

Summary of cause

AAP staff did not follow the standard procedures in relation to handling confidential information.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☐
- Financial ☐
- Legal ☐
- Reputational ☑

Description

Personal information may have been wrongly disclosed.

Severity of actual impact

Minor

Summary action plan

Reiterate to staff the appropriate steps required when handling confidential information.

Estimated Completion Date

Completed

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

Please submit Incident Report to RM Operational Risk

INCIDENT REPORT

HANDLING OF CONFIDENTIAL INFORMATION

1. SUMMARY

During Financial Administration's (FA's) BRS test on 12 January Accounting, Analysis & Policy (AAP) staff left a document containing personal staff details on a desk in the pod. This document should have been destroyed after the test. The document was found by Audit Department on 5 March when they were undertaking tests at the BRS. The document was destroyed by them at AAP's request. AAP staff have been reminded of the need to properly handle confidential information.

2. INCIDENT DESCRIPTION

On 12 January, AAP staff were working on Fringe Benefits Tax (FBT) at the BRS as part of FA's regular contingency tests. The FBT work included a three page document which showed individual payment summaries, personal addresses and reportable fringe benefit amounts. This document should have been destroyed after it was reviewed. The document was left on FA's desks in the pod when staff returned to Head Office.

Audit Department found the document on 5 March 2010 when they were at the BRS for tests. They notified the Senior Manager, AAP, who requested it be destroyed. This was done.

3. CONSEQUENCES

The consequence of this was that personal information may have been wrongly disclosed.

4. RISK REGISTER

AAP's current risk register covers this risk

Corresponding Risk Register Item	Control Description	Risk Manager	Changes to Risk Register
03b Systems and network - breach of security; unauthorised or undetected access; improper use of sensitive information	Procedures - internal and systems controls, procedures and policies, change controls. Reconciliations. Access reviews.	FA – Manager, Investments & Senior Manager, AAP	No

This incident does not relate to processes identified in FA's Business Impact Assessment.

5. ACTION PLAN

Action Description	Owner	Estimated Completion Date
Reiterate to staff the appropriate step required when handling confidential information.	Snr Manager AAP	Completed

6. SIGN OFF

Senior Manager
Accounting, Analysis & Policy

7. DISTRIBUTION LIST

Assistant Governor (Corporate Services)	Manager, AAP
Chief Financial Officer	Risk Management Unit
Senior Manager, AAP	

19 March 2010

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report to RM Operational Risk

Title of Incident Report

Loss of Confidential Electronic Data

Department(s) Compiling the Report

Domestic Markets

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
01-Jul-10	02-Jul-10	07-Jul-10	12-Jul-10

Summary description of the incident

A non-encrypted USB memory key containing confidential data was misplaced by a staff member in the The data - relate to the Bank's domestic market operations.

Summary of cause

The transport of these data has been a standard practice in for a number of years. The data are taken home each evening by the analyst assigned to duties. This practice is designed to allow domestic market operations to proceed on an informed basis in the event that the LAN fails at both HO and the BRS, and HO is inaccessible.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System ☑
- Financial ☐
- Legal ☐
- Reputational ☐

Description

Although password-protected, the lost data present a risk to the Bank, and their transport on an unencrypted USB key contravenes ST's recently implemented policies for portable electronic devices. To date, there is no evidence that the lost data have been discovered or used.

Severity of actual impact

Minor

Summary action plan

1. Arrange the purchase of an encrypted ' USB memory key for transport of confidential data.
2. Reinforce importance of data security with staff, and remind staff of responsibilities under the Bank's Code of Conduct and Data Management policies.

Estimated Completion Date

Completed

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

INCIDENT REPORT

– Loss of Confidential Electronic Data

Between 1 July and 2 July 2010, an analyst in misplaced a non-encrypted USB memory key containing confidential data. This incident report details these events, procedural weaknesses, and remedial actions taken.

Business Impact

Between the evening of 1 July 2010 and morning of 2 July 2010, an analyst in the misplaced a USB memory key containing confidential data. The loss may have occurred either at Head Office (HO), at the analyst's home, or on transport between work and home. The lost data – relate to the Bank's domestic market operations.

The data are generally at an aggregate level.

The transport of these data has been a standard practice for a number of years. The data are taken home each evening by the analyst assigned to duties. This practice is designed to allow domestic market operations to proceed on an informed basis in the event that the LAN fails at both HO and the BRS, and HO is inaccessible. These backup data have been required on rare occasions in the past.

The lost data are subject to some degree of protection, as all spreadsheets are password-protected. The usefulness of much of the data to an external party would be limited, as their interpretation requires specialist knowledge. Nonetheless, their potential discovery presents a risk to the Bank, particularly reputational, and their transport on an unencrypted USB key contravenes ST's recently implemented policies for portable electronic devices.[1]

To date, there is no evidence that the lost data have been discovered or used. As such, the actual business impact is currently classified as 'Minor'.

Risk Register

This incident relates to items 09 and 19 in the DM Risk register. The descriptions of these risks, controls and ratings are still appropriate.

Risk	Controls	Residual Risk Rating
09 – Accidental loss of records/data. Poor systems/procedures. Lack of adherence to systems.	Procedures – documented procedures/guidelines for handling electronic and other data.	Low
19 – Mis-handling of sensitive information.	Policy - Data management policies for handling and storing sensitive information, records and statistics.	Low

[1] These policies were emailed to all HO LAN users on 8 April 2010. The ST intranet site does not currently display these policies.

Business Impact Analysis

Action Items

Description	Owner	Status
Arrange the purchase of an encrypted ' USB memory key for transport of confidential data.[2]		Completed. Budget allocations for the purchase of for had been made in April, although these were not ordered at the time. Two have now been purchased for by FM Computing and are in use. procedures have been amended to require the use of an device for the transport of data. The devices can be attached to a user's keychain by a lanyard, reducing the risk of loss.
Reinforce importance of data security with staff, and remind staff of responsibilities under the Bank's Code of Conduct and Data Management policies.		Completed. E-mail sent to section staff. Section meeting to discuss other potential vulnerabilities, none identified.

Domestic Markets Department
12 July 2010

[2] ' are physically robust, and provide high level data encryption and anti-virus protection. These devices have been approved by ST for the transport of confidential information.

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report to RM Operational Risk

Title of Incident Report

Theft of RBA Blackberry 15 JUL 2010

Department(s) Compiling the Report

Economic Group, Systems & Technology

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
15-Jul-10	15-Jul-10	26-Jul-10	06-Aug-10

Summary description of the incident

An EC loaner blackberry was stolen while was on vacation The theft was immediately reported to Headquarters and the phone number disconnected; risk to the Bank is likely to be minimal. The EC blackberry has now been replaced.

Summary of cause

Burglary of the hotel room and safe.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System ☑
- Financial ☐
- Legal ☐
- Reputational ☐

Description

Very minor as access to the RBA internet through the blackberry was protected by password. Access to the phone was a risk for the few hours before the number was disconnected.

Severity of actual impact

Insignificant

Summary action plan

None.

Estimated Completion Date

26-Jul-10

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

FINAL

THEFT OF RBA BLACKBERRY 15 JUL 2010

1. EXECUTIVE SUMMARY

An EC loaner blackberry was stolen while was on vacation
The theft was immediately reported to Headquarters and the phone number disconnected; risk to the Bank is likely to be minimal. The EC blackberry has now been replaced.

2. SEQUENCE OF EVENTS

Event Time	Event Description
15.7.2010	took with him the EC loaner blackberry on vacation so he could keep up with developments at Headquarters while away. The blackberry was kept in a hotel safe when not used for work purposes. Using a crowbar, thieves broke in through the balcony door to his hotel room around 9 p.m. on 15.7.2010 and stole the entire hotel safe from the room. called headquarters three hours later (call received by) who reported the loss to a few hours later and the phone number was disconnected. The loss was reported to the police and to travel insurance company in Australia. The smashed safe was subsequently recovered on a deserted beach, minus the valuables inside (including the blackberry).

3. SYMPTOMS

Discovered by the hotel manager around 10 p.m. on 15.7.2010

4. IMPACT

Access to the RBA internet through the blackberry was protected by password. Access to the phone was a risk for the few hours before the number was disconnected.

5. CAUSE

Burglary of the hotel room and safe.

6. ISSUES

The loss will form part of the claim under travel insurance and be reimbursed to the RBA if paid by them ($500 maximum per item under the policy).

7. RISKS AND BUSINESS IMPACT ANALYSIS

With the Blackberry password protection which activates after 15 minutes of inactivity there is minimal business risk, apart from unauthorised access to the phone.

This risk relates to Risk 24 – Theft of sensitive info by media or third party. It is not envisioned that this risk should be changed or that any new risks be added to the register.

This incident also relates to Item ST-7 External Services and is rated as high. No change the ST BIA Template is required.

8. RECOMMENDATIONS

Maintain current policy of password controls for RBA Blackberry's.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
None				

10. DISTRIBUTION LIST

Name	Name	Name

11. SIGN OFF

Title	Name	Signature
ST Department Head (Acting)		

EC Dept Head