Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Misplaced / Lost Laptop - September 2008

Department(s) Compiling the Report

Financial Markets

Contact Officer

Date of Incident: 20-Sep-08

Date Incident Detected: 20-Sep-08

Date RM Notified: 24.12.08

Summary description of the incident

One of Financial Markets Laptop computers which was due to be returned at the end of it's lease, was detected as missing from the FM Computing storeroom.

Summary of cause

Not determined.

Brief description of impact

Please select the relevant impact(s)

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

Description

Financial Markets needed to pay out the residual amount for the laptop as it could not be returned to the Leasing company.

Severity of actual impact

Insignificant

Summary action plan

Re-inforced with the FM Compting team, the importance of keeping the inventory records up to date; that loan register is completed in all cases; and, ensure storeroom is adequatley secured at all times.
Current PC Inventory review procedures will be updated to better reflect the physical asset checking requirements along with the Hardcat comparison during the quarterly tests.

Estimated Completion Date

31-Jan-09

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

MISPLACED LAPTOP – SEPTEMBER 2008

One of FM's Toshiba Portege M300 laptops (Barcode RBA9000364 and Serial Number – 85026132H) which was due to be returned at the end of its lease in September 2008 has been misplaced.

The laptop was in the FM Computing secure storeroom on 3 September 2008, verified by physical inspection, in conjunction with an FM Computing inventory check.

However, when our replacement laptops were configured in the second and third week of September the misplaced laptop was no longer in the storeroom. Unfortunately, on this occasion, the loan register was not updated so there is no record of whom the laptop was issued to.

On 1 October 2008 an email was sent to all FM and Risk Management users asking them to return all Bank supplied laptops for maintenance by 10 October 2008. On 10 October 2008 a reminder was sent to all users requiring them to bring their laptops in for maintenance. During this process all laptops except the misplaced laptop were verified. The misplaced laptop was not returned to the Bank as part of this process.

Subsequently, on 5 November, the Senior Manager, Technology Services sent an email to all staff in FM and RM requesting they check home and work areas for the missing laptop – there was no response to this request.

Impact

This laptop was at the end of its leasing period and was scheduled to be returned to the leasing company at the end of September 2008. As it could not be returned, Financial Markets is required to pay the residual leasing costs of $897-50.

Risk Register

This incident relates to several risks described in the ID and DM Risk Registers - items ID 34 and DM 35 address RBA assets stored in the computer room not matching GL and/or other inventory records. Item ID 37 relates to theft of physical assets. No further changes are required to the risk registers.

Action Plan

- Following this incident, an email was sent to FM Computing staff to reinforce current procedures to ensure that the loan inventory is updated for all laptops and other equipment.
- FM Computing staff were reminded to ensure that the door to the Storeroom is locked at all times (access to the Storeroom is controlled by the Bank's security card access system and the door automatically locks when it is closed). Security guards check the door is secured as part of their nightly walk through of Level 10.
- Current PC Inventory review procedures will be updated to better reflect the physical asset checking requirements along with the comparison during the quarterly tests.

Technology Services
Financial Markets Group
24 December 2008

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Virus 11 June 2009

Department(s) Compiling the Report

ST, FM

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
11-Jun-09	11-Jun-09	12-Jun-09	22-Jun-09

Summary description of the incident

A number of calls were placed to the ST Service Desk advising of accounts being locked out. 82 user accounts were locked out and an additional 20 system related accounts. The current domain password policy is configured to lockout user accounts after incorrect password attempts. It was found that one workstation was the source of repeated attempts to log in to these accounts with password guesses which were incorrect, resulting in the lockouts. This workstation had out of date anti-virus software.

Summary of cause

A USB flash drive connected to a workstation on the RBA LAN was discovered to have the virus. When the user attached the infected USB drive, the Autorun feature of Windows automatically ran the virus on the USB drive. Even though all workstations were correctly patched, the virus ran. however because of the patching it could not propagate.

Brief description of impact

Please select the relevant impact(s)

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

Description

82 user accounts were locked out for up to half an hour, resulting in the inability to log on, or if logged on, inability to perform some functions such as browsing.

Severity of actual impact

Minor

Summary action plan

- Ensure all RBA workstations have up to date AV
- Define a process for workstations/laptops when they are added and decommissioned from the network that includes addition/deletion.
- Update procedures for regular version checking
- Develop procedure for regular updating of software, patches and anti-virus on Bank equipment used outside of HO, BRS and the branches

Estimated Completion Date

End July 2009

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

FINAL

VIRUS 11-JUNE-2009

1. EXECUTIVE SUMMARY

On 11 June 2009, a USB flash drive connected to a workstation on the RBA LAN was discovered to have the virus. This was identified after a number of calls were placed to the ST Service Desk advising of accounts being locked out. Investigations showed that a single workstation was attempting to authenticate (logon to the LAN) unsuccessfully with multiple user accounts.

The current domain password policy is configured to lockout user accounts after incorrect password attempts and as a result 82 user accounts were locked out and an additional 20 accounts consisting of generic accounts, service accounts and domain administrative accounts were also locked out. The lockout policy operated as designed.

Once the workstation causing this issue was identified it was immediately unplugged from the network and removed by ST Security for further investigation. Forensic analysis of the workstation identified symptoms that the workstation had been compromised including: event logs being deleted, new services being created, and important services being disabled. These symptoms all correspond to the known behaviour of the virus. behaviour also includes attempts to logon to multiple domain accounts using dictionary techniques.

Further analysis tracked the source of the virus to a USB flash drive that a user had plugged in to the workstation to view personal files. Analysis of the USB flash drive confirmed the presence of virus – the virus was subsequently removed from the USB drive.

The Microsoft Operating System patches had been deployed to all RBA workstations to stop the virus from propagating. is designed to stop this virus from spreading over the network however it **does not** stop the virus from operating locally. Because the virus was executed locally from the USB drive, the operating system patch did not block the virus.

However, it was also found that the version running on the workstation was out of date and did not contain the correct virus signature to detect and delete the virus. Had the version of on the workstation been current, the virus would have been detected and prevented from activating.

The risk in this instance was contained quickly and without major harm to the network. The user accounts that were locked out as a result of the virus being active were identified and all accounts were fixed within approximately half an hour.

2. SEQUENCE OF EVENTS

Event Time	Event Description
11:20am	Calls placed to ST Service Desk (CSD) notifying them of user accounts being locked out
11:25am	Server Systems – ST (SS) contacted to investigate
11:30am	SS disconnect workstation from the RBA LAN
11:41am	Security –ST (SEC) notified by suspicious activity coming from the workstation
11:45am	SEC removed the workstation for further investigation
12:10pm	All user accounts that had been locked out were restored to normal by CSD

3. SYMPTOMS

- User accounts being locked out;
- Multiple login attempts from different accounts from one workstation;

4. IMPACT

- Inability for affected users (i.e. the accounts that were locked out) to login or re-authenticate to the LAN;

5. CAUSE

- Virus introduced by an infected USB flash drive attached to an RBA workstation;
- Autorun feature of Microsoft windows automatically accessed the USB flash drive and ran the virus;
- anti-virus was not up to date on the workstation. The workstation had an old version of which is end-of-life;

6. ISSUES

- s was out of date on the PC affected. The process of keeping the network based repository of PCs and laptops data up-to-date is very manual. This allows discrepancies to occur when checking for successful roll-out of software such as

- RBA users are local administrators to RBA workstations meaning that removable media (USB drives) and software can be installed and viruses can execute with privileged rights;
- A virus can masquerade as a user initiated program and list accounts (the central LAN user information directory) allowing the attempts to logon to any LAN account;
- Autorun is turned on by default on RBA workstations – allowing the running, installation and propagation of the virus;

6.1 RELATED ISSUES

While not contributing to the current incident, the following issues could exacerbate any similar occurrences:

- There is no process in ST to ensure that Bank equipment that is used outside of HO and the branches is kept up to date in terms of patching, software versions and virus signatures. This could allow a Bank PC used externally to be infected and subsequently brought onto the Bank's network;
- FM has their own PC support team who install and generally manage the PCs for FM. There is no common definition of procedures and policies of ST and FM to ensure a consistent PC environment is maintained;

7. RISKS AND REFERENCES TO BUSINESS IMPACT ASSESSMENT

System outages as well as information leakage could cause embarrassment to the Bank as well as material loss to the Commonwealth Government due to the inability of the Bank to perform its functions. There have been major outages, both publicly and privately reported, caused by

ST Risk Register - Reputational Risk – 01 Damage to reputation.

ST Risk Register - Op/Information Technology/Performance Failure – 02 Theft due to inadequate security

ST Risk Register - Op/External/Third party – 24 Theft of sensitive information by 3rd party

It is not envisioned that these risks should be changed or that any new risks be added to the register. The "Operational Risk report - 2008-9" of ST by RM notes that "the risk of theft of sensitive information by a third party" is one of the top risks and has an unacceptable risk rating. It also notes that ST is performing further work to address the risk of unauthorised access through desktop PCs.

The relevant reference from the ST's Business Impact Analysis is the Core LAN Environment to the RBA process (ST-1). The overall criticality of this process is Vital. There are no changes to the Business Impact Analysis as a result of the incident.

8. RECOMMENDATIONS

Stopping similar viruses on the RBA network requires several layers of defence

Long term, as viruses become more sophisticated and targeted, the RBA will need to evolve its policies and technology to deal with non-RBA equipment and software being introduced into the RBA network.

In the short to near term, the following are recommended:

- Confirm all workstations have the latest version of anti-viruses and re-examine daily checking procedures to ensure total coverage;
- Introduce a periodic process to check for consistency that all workstations are patched and have up to date anti-virus
- An additional process be put in place by ST to ensure the current manual updating of the network based repository of PCs and laptops (i.e.) is up-to-date, and all relevant areas of ST are informed when workstations are added or decommissioned. Because the process is manual, there is the chance that some discrepancies will exist;

8.1 RELATED INVESTIGATIONS

In addition, there are several other avenues which will be explored although it is not clear whether they will lead to near term improvements in the risk profile:

- Investigate whether the Autorun service should be disabled on workstations. Technically this is possible, however, the full operational impact would need to be assessed;
- Removal of the ability to install and execute non-authorised software within the RBA environment. This would be likely to require some restrictions on the ability of individual users to install software on their workstations without appropriate authorisation. If viable, ST will look to develop a proposal for consideration by the RMC;
- Investigate the use of on the workstation environment – this technology could identify extraordinary or unusual behaviour on workstations and therefore helps guard against zero day attacks where anti-virus signatures are not available;
- provides access to the network for equipment that meets a designated profile such as updated anti-virus and operating system patch levels. has matured in the last few years, but previous reviews found the technology immature. However in cases such as this

i.e. virus activity due to out of date AV, would have prevented workstations joining the RBA network without up to date patches and anti-virus until they were remediated;

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Ensure all RBA workstations have up to date AV	High	High	End June 2009	Security
Define a process for workstations/laptops when they are added and decommissioned from the network that includes addition/deletion.	High	High	End June 2009	Security/ Desktop Services/ Server Systems/ CSD
Update procedures for regular version checking	Medium	Medium	End July 2009	Security
Formalise responsibilities and consistent policies and procedures to be used by ST and FM support teams	Medium	Medium	End July 2009	
Develop procedure for regular updating of software, patches and anti-virus on Bank equipment used outside of HO, BRS and the branches	Medium	Medium	End October 2009	Security/ Desktop Services
Note to all RBA staff regarding risks with USB drives	Medium	Medium	End June 2009	Security

10. RELATED INVESTIGATIONS

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
ST to investigate disabling "autorun" from all Workstations.	Medium	Medium	End August 2009	Desktop services
ST to test functionality on workstations.	Low	Low	End December 2009	Security
ST to investigate options for restricting software installation and execution.	Medium	Medium	End September 2009	Security
Review the use of technology to restrict workstation access to the LAN	Medium	Medium	End December 2009	Security/ Comms

11. DISTRIBUTION LIST

(Include the names of all persons to whom a copy of the incident report will be sent.)

Name	Name	Name

12. 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 Laptops

Department(s) Compiling the Report

ST

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
13-Aug-09	13-Aug-09		25-Nov-09

Summary description of the incident

In recent months two laptops have been stolen from the homes of ST staff members.

Summary of cause

Laptops are provided to Bank staff for out-of-hours access and for support. The laptops often remain at the home of staff members for the duration of their support cycle.

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 laptops - estimated $2600.

Severity of actual impact

Insignificant

Summary action plan

ST staff reminded not to store Bank material on local hard drives.
Bank material should only be stored on encrypted USBs.

Estimated Completion Date

15 May 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 LAPTOPS

1. EXECUTIVE SUMMARY

In recent months two laptops have been stolen from the homes of ST staff members. The total financial cost was around $2600. There is no risk of unauthorised access to sensitive data arising from these thefts.

2. SEQUENCE OF EVENTS

On Thursday 13th August 2009 an RBA laptop barcode RBA2008331 was stolen from the home of whilst he was at work. The theft was part of a general home burglary. Police were called and an event number was allocated.

On Tuesday 8th September 2009 an RBA laptop barcode RBA2006002 was stolen from the home of] whilst he was at work. The theft was part of a general home burglary. Police were called and an event number was allocated.

3. SYMPTOMS

In each case the lost laptop was identified as part of the post home-burglary inventory.

4. IMPACT

In one case the laptop was used for on-call support, while the other was made available as part of the BRS arrangements and for general access for the staff member for working on Bank material from home or while travelling. It is possible, although unlikely, that some recent ST working documents were stored on the computers. Any such documents would not contain material of a sensitive nature.

The laptops had standard software for accessing the VPN but are 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 tokens were 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 to cover both laptops, the Bank will be liable for around $2600 in total.

5. CAUSE

Support laptops are usually kept at the home of the staff member who is currently on-call. Staff who have a laptop as a desktop or for ad-hoc out of hours access, would also leave

their laptop at their homes for various periods (e.g weekends or duration short leave breaks, etc).

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, no sensitive data is known to have been stored on the laptops but this may not always be the case in future thefts. ST recently updated to the RMC on password protection of hard drives. When the documentation and safe approach are finalised a recommendation for its use across the Bank will progressed. In the interim, all ST staff will be reminded that no Bank material should be stored on the local drives of laptops that are left for periods at home. Where material needs to be stored, ST staff should use a prescribed USB which includes encryption.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Head of ST to remind staff that no Bank material to be stored on local hard drives.	Low	Med	4 Dec 2009	
ST staff to use encrypted USBs when required to store Bank material away from office.	Low	Med	15 Jan 2010[1]	

10. DISTRIBUTION LIST

Name	Name	Name

11. SIGN OFF

Title	Name	Signature
ST Department Head		

[1] This is an estimated date. As reported to the RMC, the USBs have been tested, but the vendor is yet to provide the final version of their solution.

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Accidental release of sensitive information to external contact

Department(s) Compiling the Report

Economic Analysis

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
23-Sep-09	23-Sep-09	23-Sep-09	30-Sep-09

Summary description of the incident

On 23 September, a staff member in the Regional and Industry Analysis section of EA accidently sent a sensitive internal email to an external contact. The person who received the email was an Administration and Research Assistant to the Chief Economist of an industry association (the RBA regularly speaks to this industry association as part of its business liaison program). After realising their mistake within a couple of minutes, the RBA staff member called the external recipient and asked them to delete the email, to which they agreed to straight away. The external recipient assured the RBA staff member that the information contained within the email would not be disclosed any further.

Summary of cause

Carelessness when sending an email.

Brief description of impact

Please select the relevant impact(s)

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

Description

Given the sensitivity of the document released, this incident had the potential to cause reputational damage.

Severity of actual impact

Insignificant

Summary action plan

Discuss with ST options to strengthen external email security arrangements. We could possibly move towards sending emails with only a link to an internal document, and with no actual written information contained in the email (i.e. no abstract).

Estimated Completion Date

12/10/2009

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 Description ☐
Risk Ratings ☐	New Risk ☐

Please submit Incident Report to RM Operational Risk

RISK MANAGEMENT

INCIDENT REPORT: ACCIDENTAL RELEASE OF SENSITIVE INFORMATION TO AN EXTERNAL CONTACT

Description

On the morning of 23 September 2009, an economist in the Regional and Industry Analysis (RIA) section of Economic Analysis Department (EA) accidently sent a sensitive internal email to an external contact. The email contained a 7-sentence summary of an analytical note, and a hyperlink to the full document. While the external recipient could not access the full document, the contents of the abstract were sensitive, and could have caused some reputational damage to the RBA.

The RIA economist was asked to send the email to a select list of internal staff members, but their 'autocomplete' function in Outlook added an external recipient with the same last name as one of the intended RBA recipients. The RIA economist did not check their address list before sending the email. The external person who received the email was an Administration and Research Assistant to the Chief Economist of an industry association (the RBA regularly speaks to this industry association as part of its business liaison program).

Impact

While the *potential* impact of this incident could have been significant, the *actual* impact was small. The staff member quickly recognised his mistake, and called the external recipient and asked her to delete the email, to which she agreed to straight away. I also called the Chief Economist involved to make sure that the contents of the email would not be disclosed any further. The Chief Economist indicated that he was sensitive to the problem and was well aware of the obligation of organisations like his (and the RBA) to ensure that emails received in error are deleted.

Risk Register

This incident relates to Risk 01 in the Economic Group's risk register: 'Op/Information/Disclosure–Accidental/Premature release of information. Improper release of sensitive or classified information.'

There are no changes to the risk as a result of the incident.

Business Impact Assessment

The incident relates to EC-3 Publish Data process in the Business Impact Assessment.

No changes are required as a result of the incident.

Action Plan

EA will liaise with S&T to discuss options for strengthening external email security arrangements. Another idea proposed is that EA sends emails with only a link to an internal document, and with no actual written information contained in the email (i.e. no abstract).

Head of Economic Analysis Department
30 September 2009

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Assignment of external contact to the wrong distribution list 18-Nov-09

Department(s) Compiling the Report

ST

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
18-Nov-09	24-Nov-09	25-Nov-09	8 Dec 2009

Summary description of the incident

On the 18th of November 2009 IN requested the ST Service Desk to add an external contact, . to the IN-Contacts(Media) email distribution list . By mistake ST Service Desk staff assigned this external contact to the wrong distribution list, IN-Media-Office. As the All RBA Staff distribution list is made up of other groups, the external contact was effectively also added to this group. Upon discovery on the 24th of November 2009 was removed from the IN-Media -Office group and added to the right group.

Summary of cause

The Service Desk staff performing this request selected the wrong distribution list from the search results. As the Bank has 982 groups a keyword search is used to select groups. This search produced a list where the IN-Media-Office and the IN-Contacts (Media) were presented next to each other. The wrong group was selected. It was caused by human error.

Brief description of impact

Please select the relevant impact(s)

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

Description

Potential impact was high as confidential information could have been disclosed to an external contact. All emails sent to the IN-Media-Office or All RBA Staff group were sent to the external contact,
Fortunately, no confidential data was sent using these distribution lists before the error was discovered and corrected.

Severity of actual impact

Minor

Summary action plan

The procedure for adding external contacts to the distribution list was changed to incorporate verification by the Manager, Service Desk and the Requestor and Authoriser from the business area. The request is not to be assigned a completed status until confirmation from the business area is received.
The design of the dialogue box highlighting an external destination of email will also be looked to increase its visibility, but as this is externally supplied, there will be limitations on options available.
To give users the opportunity to remove dormant lists and verify membership of the groups, the feasibility of sending distribution lists periodically to their owners for confirmation (every 3 months) will be investigated.

Estimated Completion Date

30-Apr-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

DRAFT / FINAL

ASSIGNMENT OF EXTERNAL CONTACT TO THE WRONG DISTRIBUTION LIST 18-NOV-2009

1. EXECUTIVE SUMMARY

On the 18th of November 2009 IN requested the ST Service Desk to add an external contact to the "IN-Contacts(Media)" email distribution list in the Nat&Metro Newspapers category. By mistake, ST Service Desk staff assigned this external contact to a different email distribution list ("IN-Media-Office"). The distribution list "All RBA Staff" is formed as an aggregation of other email groups. Therefore, the journalist was also effectively added to "All RBA Staff". The cause was human error. The Service Desk staff member selected the "IN-Media-Office" group which was listed immediately under "IN-Contacts(Media)" on the displayed screen of groups.

The journalist received eight "All RBA Staff" emails, along with two emails intended only for the Media Office. There was a potential risk that very confidential information could have been disclosed to the journalist Fortunately, no confidential data were sent using this distribution list before the error was reported and corrected on the 24th of November 2009.

To minimise the risk of such an error happening in the future the procedure for adding an external contact to the distribution list has been changed in order to incorporate verification by the Manager, Service Desk and confirmation by the Requestor and Authoriser from the business area.

2. SEQUENCE OF EVENTS

Event Time	Event Description
18 Nov 09 15:50	sent an email to the Service Desk requesting be added to the IN-Contacts(Media) email group under the 'Nat&Metro Newspapers' category. sent this email using the RBAInfo email box and cc
18 Nov 09 17:32	Heat call 268995 was lodged by

Event Time	Event Description
18 Nov 09 17:40	first created a new external contact To add this new contact, he then called up the list of email distribution groups, but mistakenly selected which was immediately below the intended distribution group.
18 Nov 09 17:43	sent email notification saying "added" back to
24 Nov 09 11:02	from the Service Desk received a call from stating that is receiving emails sent to the RBA staff and requested that it be investigated.
24 Nov 09 11:16	investigated this problem and found that has been added to the group. She removed him from this group immediately and added him to the email group under the category, as per the original request.
24 Nov 09 14:00	asked to request an urgent report of the specific emails sent to
24 Nov 09 15:00	notified about this incident. notified and asked for it to be investigated.
24 Nov 09 15:15	investigated this issue and provided relevant information to
24 Nov 09 16:00	initiated a revision of the procedure with and
24 Nov 09 17:00	asked to raise awareness within the Service Desk group and requested to proceed with extra caution when adding external contacts. also requested secondary verification of all updates.
25 Nov 09 08:33	provides report of emails received by to the Media Office.
25 Nov 09 9:30	The existing procedure was modified by
25 Nov 09 14:30	This incident and a modified procedure were discussed at the Service Desk group meeting. The procedure was implemented by

3. SYMPTOMS

replied to one of the emails sent to the IN-Media-Office group enquiring as to why he is receiving these emails.

4. IMPACT

Potential impact was high as confidential information could have been disclosed to an external contact. All emails sent to All RBA Staff and the group were sent to the external contact, The emails were sent over the course of one week, spanning an episode of particular sensitivity for the Media Office

Fortunately, no confidential data were sent using these distribution lists before the error was discovered and corrected.

5. CAUSE

The Service Desk staff performing this request selected the wrong distribution list from the search results. As the Bank currently has email groups, the keyword search is used to find an appropriate group. The search produced a list where the and the were displayed immediately next to each other. The wrong group was selected and the add button pressed. The cause of the incident was human error.

6. ISSUES

At the time of the incident the Service Desk procedure for adding external or internal contacts to email distribution lists were the same. The procedure did not provide for secondary verification by other Service Desk staff or confirmation by the business area to mitigate the risk caused by assigning a contact to the wrong group.

7. RISKS AND BUSINESS IMPACT ANALYSIS

This incident relates to the following risk in the ST Risk Register.

- Risk 14 Op/Information/Disclosure – Staff release data belonging to the Bank to third party who is not entitled to see it. Accidental or deliberate internal disclosure or ignorance of legislative requirements eg. Improper use of personal or sensitive information such as payroll.

It is proposed to update ST Risk Register to add following control:

Change procedure for adding external contacts to the distribution list to incorporate verification by Manager, Service Desk and confirmation by Requestor and Authoriser from the business area.

8. RECOMMENDATIONS

It is recommended that the procedure for adding external contacts to the distribution list should be changed to incorporate verification by the Manager, Service Desk. Furthermore, the screen print displaying the distribution list's membership should be sent to the Requestor and Authoriser from the business area. The request is not to be assigned a completed status in the Service Desk system until confirmation from the business area is received.

In addition, the feasibility of sending distribution lists periodically to their owners for confirmation (say every 3 months) should be investigated. While this would not directly assist with the current incident, it would give users an opportunity to remove dormant lists and verify membership.

Finally, the dialogue box alerting users that they are sending an email externally will be looked at to see if it can be redesigned to make warnings more prominent. However, this dialogue box is part of externally supplied software and there will be limitations on what options are available.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Modification of 'Creation/ Editing of Distribution Lists' procedure	High	1	Completed	
Implementation of modified procedure to provide for secondary checking in Service Desk and confirmation by requesting business area.	High	1	Completed	
Investigate feasibility of periodically sending distribution lists to their owners for confirmation (say every 3 months).	Medium	2	End of April 2010	Senior Manager, Service Management & Desktop Support

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Investigate redesign of the dialogue box alerting users that they are sending an email externally. During the investigation an implementation timeline will be agreed with vendor.	Medium	2	End-January 2010	Senior Manager Security

10. DISTRIBUTION LIST

(Include the names of all persons to whom a copy of the incident report will be sent.)

Name	Name	Name

11. SIGN OFF

Title	Name	Signature
ST Department Head		

ADDENDUM TO INCIDENT REPORT

Assignment of external contact to the wrong distribution list – 18 November 2009

Reference to Business Impact Analysis assessment

This incident relates to the provision of email services and is covered in ST's Business Impact Analysis – Core LAN environment to RBA process (ST-1). There are no changes to ST's Business Impact Analysis as a result of the incident report.

Systems & Technology Department
8 December 2009

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

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 laptop between Craigieburn and Head Office

Department(s) Compiling the Report

Note Issue

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
08-Nov-10	17-Nov-10	24-Nov-10	01-Dec-10

Summary description of the incident

ST requested that a faulty laptop in Craigieburn be returned to Head Office for repair. NI arranged through IN for courier service to collect the laptop from Craigieburn on 4/11/10 (consignment number The laptop was identified as missing on 17/11/10. last scanned the package on 8/11/10. When notified, undertook to investigate. The laptop was found at Greenacre, NSW on 23 November by a member of the public, who contacted the Bank. ST collected it on the same day. ´ were contacted and informed the laptop had been recovered.

Summary of cause

Incident caused by external courier. Investigation pending.

Brief description of impact

Please select the relevant impact(s)

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

Description

Financial loss if the laptop was not recovered.
Reputational damage if sensitive information was stolen from the laptop. Mitigating this risk, however, the laptop hard drive was password protected and forensic analysis confirmed that the hard drive had not been accessed. RMU Category: Op/Physical Security/Safeguarding physical assets.

Severity of actual impact

Insignificant

Summary action plan

ST to inform once the laptop has been recovered (completed 23 November). Discuss the incident with to establish the procedural changes required to prevent the reoccurance of this incident (December 2010). IN to place packaging guidelines on the intranet for Bank-wide reference.

Estimated Completion Date

December 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 Description ☐

Risk Ratings ☐ New Risk ☐

INCIDENT REPORT

LOSS OF LAPTOP BETWEEN CRAIGIEBURN AND HEAD OFFICE

ST requested that a faulty laptop in Craigieburn be returned to Head Office for repair. was engaged to courier the laptop. The laptop went missing, whilst in possession, prior to delivery to Head Office.

The Incident

NI Craigieburn staff requested Head Office Mail Room to arrange for courier service to collect faulty laptop from Craigieburn on 4 November 2010 (consignment number). The laptop was packaged in a padded laptop bag and then placed in a Toshiba laptop box that was previously used by ST to transport the laptop from Sydney to Craigieburn.

The laptop was identified as missing on 17 November 2010. was immediately contacted and they advised that while the laptop had reached the depot in Sydney, delivery to the Bank was delayed due to an incident on the road (enquiry reference number . also advised that couriered items are scanned on a daily basis and the laptop was last scanned on 8 November and therefore had not been tracked for nine days.

undertook to investigate and provided daily updates to NI. On 22 November, told the matter was escalated to security for security footage to be reviewed.

At 8am on 23 November, contacted to advise that the laptop had been found by a member of the public in Greenacre, NSW. The gentleman had contacted the Reserve Bank who in turn contacted ST. When found, the laptop was no longer in the outer shipping box. However, it was still in the laptop bag along with the power cord.

TNT was informed that the laptop had been found. ST has examined the laptop and has confirmed that the laptop does not appear to have been accessed. ST has also identified a number of files on the laptop.

Procedural Adherence

Head Office Mail Room arranged to use the Bank's preferred courier as per the procedures, and the hard drive was password protected. While the procedures for organising a courier were adhered to, NI staff were not aware of IN's packaging guidelines.

Risk Assessment

The incident may have led to the following risk impacts:

- Financial loss if the laptop was not recovered; and
- Reputational damage if sensitive information was stolen from the laptop. Mitigating this risk, however, the laptop hard drive was password protected.

Action Plan

- ST to inform once the laptop has been recovered (completed 23 November).
- Arrange a meeting between and (IN) and appropriate representatives to discuss how this incident occurred and what will be changed to ensure that the incident is not repeated (December 2010).
- Arrange for IN to make available their packaging guidelines (IN provided these guidelines to NI on 24 November. A further request to make these guidelines more widely available was made on 29 November).

Research and Development
Note Issue Department
29 November 2010

\\\san2\bsgdata\ni\risk control\risk management\incident reports\2010 11 23 - missing laptop.docx

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report to RM Operational Risk

Title of Incident Report

Accidental loss of information

Department(s) Compiling the Report

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
23-Nov-10	23-Nov-10	24-Nov-10	06-Dec-10

Summary description of the incident

A folder containing information prepared for a meeting was accidently left on the boot of the office car while we were preparing to leave the car park of We were advised by a passing motorist that we had dropped the folder when we had joined traffic. On return to the car park we found papers scattered over the road and wind gusts had taken some of the papers 100 metres up the road. We spent one hour searching for papers along the road. Most of the scattered documents were located.

Summary of cause

Staff member was distracted and did not notice folder on the boot of the car.

Brief description of impact

Please select the relevant impact(s)

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

Description

Staff collected scattered material from the road (paying due care and attention to physical safety).

While most information was recovered, two documents have been lost which contain confidential information. We suspect that these documents have fallen into storm water drains.

Severity of actual impact

Moderate

Summary action plan

In response to this incident we plan to take only limited confidential information to future meetings.

Estimated Completion Date

NA

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 ☐

RISK MANAGEMENT

INCIDENT REPORT: ACCIDENTAL LOSS OF INFORMATION

Description

Around 1pm on 23 November 2010, documents (three pages) were lost The incident occurred during a visit attended by two staff members.

A folder containing information prepared for a meeting was accidently left on the boot of the office car while the staff were preparing to leave the car park of The staff member involved was distracted and did not notice folder on the boot of the car.

Staff were advised by a passing motorist that material had fallen from the car when they had joined traffic. On return to the car park staff found papers scattered over the road and wind gusts had taken some of the papers 100 metres up the road. The staff spent one hour searching for papers along the road Most of the scattered documents were located.

Impact

The potential impact of this incident could have been significant. However, staff were able to recover most of the information which had been lost. Staff collected scattered material from the road and surrounding properties paying due care and attention to physical safety.

While most information was recovered, two documents have been lost which contain confidential company-specific information. Other documents of a non-confidential nature were found lying at the bottom of a storm water drain. Staff suspect that the confidential documents have also fallen into storm water drains, resulting in a moderate reputational risk to the Bank.

Risk Register

This incident relates to 01 in the risk register.

No changes are required as this risk is already captured under Control Description Procedures well understood by staff.

Business Impact Assessment

This incident relates to EC-5. No changes are required.

Action Plan

Staff will review the need to take confidential information on visits.

6 December 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 Personal iPad Containing a Bank Presentation

Department(s) Compiling the Report

Note Issue

Contact Officer

.

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
26-Nov-10	26-Nov-10	01-Dec-10	01-Dec-10

Summary description of the incident

On 26 November 2010, following a cancelled flight from Melbourne to Sydney, personal iPad was lost. The iPad contained a copy of the presentation gave to the ICCOS Conference, along ~~with~~ the agenda/itinerary and a work program.

Summary of cause

While having an electronic copy of the presentation and work program on personal iPad is not prohibited by the Bank, it does highlight a security risk. The risk could have been mitigated somewhat if the iPad had been locked.

Brief description of impact

Please select the relevant impact(s)

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

Description

Effort in arranging a remote wipe of the iPad to return the device to a clean state.

RMU Category: Op/ Information/Disclosure.

Severity of actual impact

Insignificant

Summary action plan

1. iPad's with Bank-related information be locked; and
2. continues to monitor Qantas lost property and the status of the iPad wipe.

Estimated Completion Date

December 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 ☐

INCIDENT REPORT

LOSS OF PERSONAL IPAD CONTAINING A BANK PRESENTATION

On 26 November 2010, following a cancelled flight from Melbourne to Sydney, personal iPad was lost. The iPad contained a copy of the presentation gave to the ICCOS Conference, along with the agenda/itinerary and a work program.

Incident

In preparation for his trip to the ICCOS Conference in Malaysia, copied the presentation onto his personal iPad, to provide an opportunity for preparation on the flight. In addition, the itinerary, and agenda were loaded, along with a copy of some work program ideas (Attachment One).

On 26 November, travelled to the NNPDC to escort a visitor from the on a tour. flight back was at 1730, but due to weather delays, the plane stayed on the tarmac until it was cancelled around 2100. When disembarking the plane, it appears that left the iPad on the plane.

Remedial Action

On discovering the iPad was missing, returned to the gate, but no staff were available to assist. then arranged for a remote wipe of his iPad, which is designed to return the device to a clean state. The wipe will occur when the iPad is next connected to a wifi network. As at 8am on 30 November, the iPad had not been connected. contacted Qantas lost property in Melbourne and Sydney on 29 November, but the device had not been handed in (lost property does not open on weekends).

Procedural Adherence

While having an electronic copy of the presentation and work program on personal iPad is not prohibited by the Bank, it does highlight a security risk. The risk could have been mitigated somewhat if the iPad had been locked.

Risk Assessment

The material on the iPad is in a PDF format, and could be copied from the device and circulated. The presentation was given to a commercial and central bank audience, and copies of the presentation in PDF format will be distributed to delegates. The dissemination of the agenda/itinerary pose few risks. The work program does not contain confidential information, but does show ideas that DP staff are considering.

Action Plan

It is recommended that:

- iPad's with Bank-related information be locked; and
- continues to monitor Qantas lost property and the status of the iPad wipe.

Note Issue
30 November 2010

Graph – Similar to the processing graph in presentation but can we estimate total processing (CIT plus RBA). Can we base it on lodgements?

Diary note – Can we get a picture of movements to / from CITs by banks and RBA?

Graph – Banknotes destroyed per capita versus banknotes in circulation per capita.

You need to do a presentation for Five to ten minutes focusing on the strategic objectives / achievements of our commercialised model.

- Stacking issue –

Has specified a forecast model where currency is a function of prices and GDP? How does this compare to the simple growth rate assumptions

Diary Note : Literature search

(1) Examine possibility If there is a problem then the charge applies back to the previous audit!!!

Should we segregate new banknotes out of VCH, ie only payout on banknotes have been processed.

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 Bank Document Containing Sensitive Information

Department(s) Compiling the Report

Note Issue

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
07-Feb-11	07-Feb-11	28-Feb-11	28-Feb-11

Summary description of the incident

On 7 February 2011, a Bank document containing sensitive information was carried onboard a flight from Sydney to Melbourne by and was lost in transit.

Summary of cause

While carrying and reading work-related documents outside of the Bank premises is not prohibited by the Bank, it does highlight a security risk.

Brief description of impact

Please select the relevant impact(s)

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

Description

Notwithstanding the effort spent in trying to retrieve the document, the risk of the paper ending up in the hands of a person who might benefit directly from the information is considered to be low.

This incident relates to risk #NG02 'Inappropriate or unintentional disclosure of confidential information' in the NI risk register.

Severity of actual impact

Minor

Summary action plan

No specific action items arose from the incident. However, the incident provides an opportunity to review the policy which permits staff to travel with documents containing sensitive information. At the very least, Bank staff will be reminded that care should be taken when carrying and reading work-related documents during travel.

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 ☐

INCIDENT REPORT

LOSS OF BANK DOCUMENT CONTAINING SENSITIVE INFORMATION

On 7 February 2011, a Bank document containing sensitive information was carried onboard an aircraft by and lost in transit.

Incident

During the flight from Sydney to Melbourne on the way to NPA, accessed his bag a number of times to read several Bank documents. When the aircraft reached its destination, checked his bag and realised that one draft discussion paper that he had read, was missing. searched the pocket attached to the seat in front, as well as the surrounding areas (seats and floor), but could not locate the paper.

Remedial Action

Several attempts to retrieve the paper were unsuccessful. As soon as disembarked from the aircraft, he unloaded the contents of his bag to check whether the paper had slipped in between other documents. then went to the baggage claim area with a view to querying the passenger who was seated next to him (who also had a handful of documents on board); however, the attempt to locate the passenger was unsuccessful. returned to the gate to seek the assistance of airport crew, who went into the aircraft to conduct a brief search. On 8 and 11 February, enquired with the Qantas Melbourne Lost & Found Property Office, and on 10 February, the Sydney and Perth offices, given that the aircraft had also flown to these cities subsequent to the incident.

Procedural Adherence

While carrying and reading work-related documents outside of the Bank premises is not prohibited by the Bank, it does highlight a security risk. The risk could have been mitigated had not accessed multiple documents at the same time during the flight.

Risk Assessment

Although the draft discussion paper does not contain highly sensitive Bank information, or any third party confidential information, it does present an evolution of ideas. However, given the environment and circumstances under which the incident occurred, the risk of the paper ending up in the hands of a person who might benefit directly from the information is considered to be low.

Action Plan

No specific action items arose from this incident. However, the incident provides an opportunity to review the policy which permits staff to travel with documents containing sensitive information. At the very least, Bank staff will be reminded that care should be taken when carrying and reading work-related documents during travel.

Note Issue Department
25 February 2011

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report to RM Operational Risk

Title of Incident Report

Loss of RBA Blackberry 30/03/2011

Department(s) Compiling the Report

Economic Group

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
30-Mar-11	30-Mar-11	31-Mar-11	07-Apr-11

Summary description of the incident

was transferring from a flight at Bangkok to check in . In leaving the plane quickly for the next flight he left his Blackberry on the flight. Within ten minutes he realised and notified s (as he wasn't allowed back to the plane). reported the Blackberry couldn't be located.

Summary of cause

Blackberry was left on a plane.

Brief description of impact

Please select the relevant impact(s)

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

Description

Minor risk of access to RBA mail and intranet, or use of phone, as the Blackberry was password protected (including to make calls). Phone was disconnected within hours. The loss of equipment was estimated as $700.

Severity of actual impact

Insignificant

Summary action plan

None

Estimated Completion Date

Closed

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 ☐

Loss of RBA Blackberry – 30 March 2011

1. Executive Summary

A Blackberry was left by on flight TG 478 from Sydney to Bangkok, departing at 1625 on Tuesday 29 March 2011 and arriving into Bangkok at 2155.

2. Sequence of Events

took his RBA blackberry with him to attend a conference
In his rush to check in for the connecting flight (one km from the arrival gate) he left his blackberry on the Thai flight. A few minutes after getting off he realized he had left it but he couldn't go back. asked airport staff to check on the plane and was told it wasn't there. emailed at 3am on 30 March to report the loss. It was reported to ST Service Desk and Travel Department at 9.15 on 30 March. ST put a hold on the number so the phone could not be used unless they reactivated it. The loss was reported to Risk Management Unit on 31 March.

Also on 31 March contacted Thai Airways Customer Service who investigated and wrote back on 1 April to say the phone had not been found or handed in at lost property. ST was notified on 4 April that the phone was officially lost.

3. Symptoms

Loss discovered by after leaving the plane in Bangkok Airport.

4. Impact

Access to the RBA internet through the Blackberry was protected by password. Access to the phone was at risk for the few hours before ST put a stop on the phone number.

5. Cause

RBA Blackberry left on the plane.

6. Issues

The Bank is not insured for loss of equipment such as this. The loss to the Bank is estimated as $700.

7. Risks and Business Impact Analysis

With the Blackberry password protection there is minimal business risk.

This risk relates to Risk 10 – Unauthorised use/ theft of data, by internal and external users. It is not envisaged that this risk should be changed or that any new risks should be added to the register.

This incident is not related to any process in the BIA.

8. Recommendations

Maintain current policy of password controls for RBA Blackberries.

9. Action Plan

None.

10. Distribution List

11. Sign Off

Head of Economic Research Department

INCIDENT REPORT

PROVISION OF HIGH RESOLUTION BANKNOTE IMAGES TO

The Incident

a website developer, has been retained by the Bank to develop a banknotes-related micro-site.

On 23 June 2011, as part of the development work underway, a DVD containing a variety of images, including images of banknotes, was sent by courier to for use by its designers. This DVD contained banknote images of a resolution quality greater than 72 dpi. The Bank's reproduction guidelines state that banknote images greater than 72 dpi should not used by outside parties. There were 249 images on the DVD, of which 160 were high resolution partial or full images of banknotes.[1]

This incident resulted from a misunderstanding by the staff member involved regarding the application in this case of Note Issue's reproductions guidelines and an error of judgement relating to the action that was taken. The incident also highlights that more stringent checking of images that leave the department may be needed.

Remedial Action

Upon realising the error that had been made, Account Director was immediately contacted to inform him that certain images on the DVD should not have been sent to the company and to request that any images placed onto company servers and computer drives be deleted. Digital Producer subsequently advised that no copies of any images had been made, and that the DVD had not been used in any way.

The incident was also immediately drawn to the attention of the Senior Manager, Communication and the Head of Note Issue.

The following morning a Note Issue staff member retrieved the DVD from where it had been stored in a locked drawer. It was still in its unopened courier packaging, indicating that the DVD had not been used.

All External Relations team members have been reminded of the reproductions guidelines and that no high resolution images of banknotes are to be provided to outside parties without prior consultation with senior management.

Risk Assessment

In the period between 23 June and 5 July, there was a risk that high resolution banknote images could have been copied, stored and potentially misused by staff members or by other outside parties via contacts with This could have had reputational consequences for the Bank.

Remedial action taken together with the confidentiality arrangements in place with has satisfactorily mitigated this risk.

A review of Note Issue's risk registers indicated that the risk of contravention by Note Issue of its own reproduction guidelines without the prior approval of senior management is not covered. A new risk entry will be created in the NI - General Operations Risk Register.

---

[1] For the purpose of this note, 'low quality' images are defined as those of 72 dpi or less, and 'high quality' images are defined as those with dpi great than 72.

Action Plan

To further mitigate the risk of inadvertently supplying high resolution images to other parties, the following actions have been identified:

- Counsel staff involved in the need to ensure that senior management is consulted prior to taking any actions that would be outside established policy or guidelines (completed).
- Establish arrangements to remind External Relations staff periodically through the annual risk review process of the reproduction guidelines (completed).
- Manager, External Relations to check all images sent to other parties in terms of the reproductions guidelines (ongoing).
- Review naming convention of image files to ensure clear labelling of resolution status (end July 2011).
- Create a new risk entry in the NI - General Operations Risk Register that documents the risk of Note Issue contravening its own reproductions guidelines without the prior approval of senior management (end July 2011).

External Relations
Note Issue Department
7 July 2011

INCIDENT REPORT

UNINTENTIONAL DISCLOSURE OF EMAIL ADDRESSES

On 14 July 2011, an email was sent to individuals who had requested an electronic copy of the 2011 numismatic order form. Customers' email addresses were included in the 'CC' field instead of the 'BCC' field, unintentionally making the email addresses visible to all recipients.

Background

NI maintains a database of individuals and businesses wishing to receive copies of the numismatic order form, which is available in physical and electronic formats. Preceding the commencement of a numismatic banknote sale, NI staff send an email with an attached electronic copy of the order form to prospective customers who requested an electronic copy. The email addresses in the database are placed in the 'BCC' field to ensure that email addresses are not made visible to the entire group of recipients.

The Incident

The email, sent on 14 July 2011 in preparation for the 2011 sale, was sent to prospective customers as per accepted procedures. The email addresses, however, were placed in the 'CC' field instead of the 'BCC' field, making the email addresses visible to all of the email recipients. NI Enquiries received two separate emails from customers on the morning of 15 July 2011 advising that, as a result of making the email addresses visible to all recipients, the Bank was in breach of its privacy obligations.

Remedial Action

Upon realising the error, NI staff notified the Manager, External relations, who in turn notified the Head of Note Issue and the Bank's General Counsel. An apologetic email, drafted with the aid of the General Counsel, was sent to the two individuals who commented about the breach of their privacy with the reassurance that administrative procedures that led to this error would be reviewed.

Risk Assessment

The *Privacy Act 1988* prohibits the disclosure of personal information that could identify an individual, without consent of that individual. In this instance, External Relations staff unintentionally disclosed a number of private email addresses. However, an email address alone does not provide sufficient information to allow the identification of an individual. As such, it is not clear if legislation was breached. Notwithstanding the risk of breaching privacy legislation, complaints were received from only two of the 94 email recipients in this case. The Bank's reputation was therefore unlikely to have been adversely affected to any noticeable degree.

Action Plan

Staff have been counseled to take more care when sending emails in future.

Note Issue Department
25 July 2011

RESERVE BANK OF AUSTRALIA

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report by email to 'RM Operational Risk'

Title of Incident Report: Coombs Inventory Discrepancy

Reference Number *(issued by RM upon notification)*: 2011034

Department(s) Compiling the Report: FY

Contact Officer:

Date of Incident	Date Incident Detected	Date RM Notified	Date Report Submitted to RM Operational Risk
16-Jun-11	16-Jun-11	20-Jun-11	26-Jul-11

Summary description of the incident

On Thursday 16 June 2011, the Acting Coombs Administrator, : , completed the May accounts reconciliation and discovered a variance of approximately $2,000 above the Projection 2 figures. It was found that $2,757.25 was paid for replacement linen; delivery of the linen to Coombs confirmed by a despatch docket held by the supplier but there was now no evidence of these items being at Coombs.

Summary of cause

The items were removed from site without authority.

Actual impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational *(Business process/System/Information)* ☑
- Financial ☐
- Legal and Compliance ☐
- Reputational ☐

Description of Actual Impact

The reconciliation of the discrepancy and retrieval of the goods diverted resources from other tasks

Severity of actual impact: Minor

Summary action plan

1. Re-state procedures to ensure staff ordering goods or services can not approve the payment of the subsequent invoice.
2. Reinforce with : staff the importance of maintaining documentation to ensure that all orders are supported by proper authorisation from the Coombs Administrator prior to the order being placed.
3. AD requested to undertake an audit of GL transactions for the previous 3 years to identify any further anomalies.

Estimated Completion Date: 15-Jul-2011

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 ☐

FACILITIES MANAGEMENT DEPARTMENT
INCIDENT REPORT FORM

INCIDENT NUMBER:	*47*
RM Incident Number	2011034
ACTUAL IMPACT OF INCIDENT	*Minor*

Coombs Inventory Discrepancy – 16 June 2011

Reporting Officer Name and Contact Details

Senior Manager Property Services –

Incident Description
(Include time, date, sequence of events, names and contact details of those involved)

Summary

On Thursday 16 June 2011, the completed the May accounts reconciliation and discovered a variance of approximately $2,000 above the Projection 2 figures. It was found that $2,757.25 was paid for replacement linen; delivery of the linen to Coombs confirmed by a despatch docket held by the supplier but there was now no evidence of these items being at Coombs.

The Head of FY contacted who advised that had received the goods, they were incorrect and had sent them back to the supplier. The supplier subsequently advised that none of the goods had been returned or exchanged. then confirmed that "had tracked it down", the goods had gone to an old address and would be redirected to the Bank.

The matter was discussed with AG(CS) and RM on Friday 17 June and with the NSW Police by the Head of FY that afternoon.

The goods were returned to the Coombs on Monday 20 June.

The Police attended the Bank to take statements and on Tuesday 21 June, were provided with relevant documentation. On 28 June the NSW Police advised the Bank that the return of the goods would make it difficult to prove They have created a case file and assigned event number to the incident but do not propose to take any further action.

Separately AD were requested to undertake an analysis of relevant GL transactions for the previous 3 years to identify any other anomalies. The AD methodology identified another 33 transactions, all of which were investigated and subsequently found to be legitimate.

Is this potentially a Comcare Reportable Incident? No

Reference to Business Impact Analysis assessment

This incident does not relate to any key processes identified in FY Business Impact Analysis. There are no proposed changes to the Business Impact Analysis as a result of the incident.

Risk Implications

Potential fraud and theft of Bank property.

Existing Risk Treatment Controls (if any)

1. must obtain approval from the before an order for goods or services can be placed.
2. must obtain approval from the before an order for goods or services can be placed.
3. is typically not involved in ordering goods and services, but must approve the order and approve the invoice for payment.
4. A declaration that the account has been checked, goods have been received or work performed and that the account has not previously been paid is provided prior to payment by the .
5. Clear segregation of duties between manager responsible for approving the invoices, and FA Accounts Payable making the payment.
6. Monthly budget reconciliation process includes review of posted transactions and investigation of discrepancies.

Issues:

Unauthorised removal of Bank property from the Coombs Centre.

Proposed Remedial Action

Proposed Risk Treatment Measure	Person Responsible	Deadline	Priority H/M/L
1. Re-state procedures to ensure staff ordering goods or services can not approve the payment of the subsequent invoice.	LG	30 June 2011 Complete	H
2. Reinforce with staff the importance of maintaining documentation to ensure that all orders are supported by proper authorisation from the prior to the order being placed.	LG	30 June 2011 Complete	H
3. AD requested to undertake an audit of GL transactions for the previous 3 years to identify any further anomalies.	AD	15 July 2011 Complete	H

Risk Register Assessment

Remedial Action Item	Corresponding FY Risk Register Item(s)	Changes to Risk Register
1 & 2	F2	nil

Incident report and remedial Action Plan:	
Sighted:	Responsible Manager
Sighted:	Senior Manager (Security)
Sighted:	Head of FY
RM Notified:	Head of FY
Proposed Remedial Action Reviewed:	"Peer" Manager
FY Risk Register Reviewed:	Senior Manager (Security)
Remedial Action Completed:	Responsible Manager
Remedial Action Completed:	"Peer" Manager
Incident "closed":	Head of FY

D11/111108

RESERVE BANK OF AUSTRALIA

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report by email to 'RM Operational Risk'

Title of Incident Report: Targeted Email Virus Attack 17 Nov 2011

Reference Number *(issued by RM upon notification)*: 2011066

Department(s) Compiling the Report: ST

Contact Officer:

Date of Incident	Date Incident Detected	Date RM Notified	Date Report Submitted to RM Operational Risk
17-Nov-11	17-Nov-11	17-Nov-11	30-Nov-11

Summary description of the incident

A targeted malicious email was sent to several Bank staff, including senior management up to Head of Department. The email was purported to be from regarding "Strategic Planning FY2012. The malicious payload was an Internet URL link to a zip file containing a trojan which at the time, was not detectable by the Bank's Anti Virus scanners. The six users that clicked on the link had their PCs isolated until such time the AV vendors could deploy updated virus definitions. By close of business, the definitions were updated and over night virus scans were scheduled. Of note, all of the affected PCs did not have local administrator rights. This prevented the virus from spreading.

Summary of cause

Malicious email was highly targeted, utilising a possibly legitimate external account
It included a legitimate email signature and plausible subject title and content. As the email had no attachments, it bypassed existing security controls, allowing users to potentially access the malicious payload via the Internet.

Actual impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational *(Business process/System/Information)* ☑
- Financial ☐
- Legal and Compliance ☐
- Reputational ☐

Description of Actual Impact

Users with affected PCs were disrupted whilst replacement PCs were organised.
Bank assets could have been potentially compromised, leading to service disruption, information loss and reputation.

Severity of actual impact: Minor

Summary action plan

Deploy updated virus signatures from Completed.
Update email block profile to scan for embedded hyperlinks that host files/applications. - Completed.
Investigate blocking the download of all known executable application file types via the Web Browsing infrastructure. - RMC Feb 2012.

Estimated Completion Date: Feb 2012

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 ☐

TARGETED EMAIL VIRUS ATTACK 17-NOV-2011

Risk Management Unit Reference Number: 2011066

1. EXECUTIVE SUMMARY

On Wednesday 16th and Thursday the 17th of November the Bank received suspicious emails purporting to be sent from regarding "Strategic Planning FY2012". The recipient list included several Bank staff, including senior management up to Head of Department. The emails were analysed by ST Security Analysis and found to be malicious in nature.

The malicious payload was found to be a compressed zip file containing an executable malware application. The email had managed to bypass the existing security controls in place for malicious emails by being well written, targeted to specific Bank staff and utilised an embedded hyperlink to the virus payload which differs from the usual attack whereby the virus is attached directly to the email. Of note was that antivirus which is used on Bank workstations and servers did not detect this virus. The issue was escalated to several anti-virus vendors used by the Bank to ensure updated antivirus definitions were created to detect the virus.

It was also found that six users had clicked on the malicious link, potentially compromising their workstations.

ST Head of Department authorised the shutdown of all affected PCs and server until appropriate anti-virus detection and removal capabilities were created. Affected staff were individually notified by ST and FMG Computing. By close of business on the 17th of November, had committed to deploying updated virus definitions that evening. These were released and have been installed at the Bank. All affected PCs have been cleansed and returned to normal operation.

Of note, all of the affected PCs did not have local administrator rights. This prevented the virus in this case, from spreading around the network.

2. SYMPTOMS

- Suspicious email purporting to be from was sent to select Bank staff with a subject heading "Strategic Planning FY2012"
- Email was forwarded to System Security management for further analysis
- Email was found to be linking to a malicious payload on the Internet – subsequent scans revealed the threat was currently undetectable by the workstation antivirus and the server antivirus
- Further analysis showed 6 Bank staff members had potentially opened the malicious payload – these servers were considered compromised and removed from the network

3. IMPACT

- Users with affected PCs were disrupted whilst replacement PCs were organised
- Bank assets could have been potentially compromised, leading to service disruption, information loss and reputation

4. CAUSE

- Malicious email was highly targeted, utilising a possibly legitimate external account purporting to be a senior Bank staff member. It included a legitimate email signature and plausible subject title and content
- As the email had no attachments, it bypassed existing security controls, allowing users to potentially access the malicious payload via the Internet browsing infrastructure

5. ISSUES

- No automatic discovery by the mail filtering software at that time, for these types of malicious emails.
- Workstation and Server assets were potentially exposed as the required virus definitions did not exist for this particular threat
- While users are aware of the need for caution with suspicious attachments, such awareness is unlikely to protect the Bank from credible looking emails and attachments

6. RISKS AND BUSINESS IMPACT ANALYSIS

- STR2005 – Malicious externally generated attack or act of sabotage.

There are no recommended changes to this risk in the risk register. There are also no recommended changes to the BIA ST template.

7. RECOMMENDATIONS

- Deploy updated virus signatures from
- Update the block profile to scan for embedded hyperlinks in emails that link to known applications/executables. Emails that have links to Internet hosted files/application will be automatically blocked and require ST Security review.
- Consider blocking the download of all known application files (including zip files) via the Web Browsing infrastructure. Where necessary, an exception list can be made for specific business units whilst keeping the overall exposure to a minimum.

8. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
	Low	High	Completed	Security Analysis – ST
Update] email block profile to scan for embedded hyperlinks that host files/applications.	Low	High	Completed	Security Analysis – ST
Investigate blocking the download of all known executable application file types via the Web Browsing infrastructure.	High	Medium	RMC – 1 Feb 2012	Security Analysis - ST

9. DISTRIBUTION LIST

Name	Name	Name

10. SIGN OFF

Title	Name	Signature
ST Department Head		

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report to RM Operational Risk

Title of Incident Report

Inadvertent release of internal document related to the tender to an external party

Department(s) Compiling the Report

FA

Contact Officer

Date of Incident

Date Incident Detected

Date RM Initially Notified

Date Report Submitted to RM

Summary description of the incident

The evaluation methodology document for the tender was inadvertently sent via e-mail to an external party who had previously requested a copy of the tender. This occurred when the evaluation methodology was being internally circulated for review and comments.

Summary of cause

Insufficient review of e-mail addresses prior to sending.

Brief description of impact

Please select the relevant impact(s)

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

Description

This error may have reputational and legal consequences as the probity of tender may be questioned if the Bank had not responded to the error. One component of the tender has been delayed.

Severity of actual impact

Minor

Summary action plan

The recipient of the document has been asked to delete the email, the attachment and any saved copies, and confirm via email that this has been done. The recipient has confirmed the deletion as requested. The section of the tender for which the company was interested in has been withdrawn. Project staff have been reminded of the importance of properly reviewing email addresses. Email groups have been established to ensure that e-mail addresses need not be re-entered each time an e-mail is to be sent to the evaluation committee.

Estimated Completion Date

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

Inadvertent release of internal document to external party on

1. SUMMARY

On a document meant only for internal distribution was accidentally sent to an external party. The document contained the proposed methodology for evaluating the tender. Outlook's auto-complete function included a previously entered email address for a potential bidder. This was not detected before the email was distributed. The external recipient of the email has been contacted and asked to delete the email, the attachment and any saved copies, and the Bank has received an email confirming that this has been done. The specific section of the tender that the external party was interested in has been withdrawn until a later date. Project staff have been reminded of the importance that emails are correctly addressed. Email groups have been created so that there is no need to enter individual email addresses each time an email is to be circulated.

2. DESCRIPTION

The evaluation methodology document was to be internally circulated on Friday, for review and comments on the proposed weightings given to factors for evaluate competing tenders.

The project officer had been responding to requests for the tender documents since the release of the tender on AusTender from an email mailbox specifically established for the project. The evaluation methodology document was sent from the standard work email mailbox. The project officer incorrectly believed Outlook's auto-complete function has separate address lists for each mailbox. It maintains a single list for all boxes. When the project officer entered to send the message to Outlook added an external party to the email instead. The email was sent without the wrong address being detected. As a result the document was inadvertently sent to an external party.

3. CONSEQUENCES

Risk 10 OP/Information/Disclosure in FA's risk register states that the consequences for this type of event are reputational and legal. If action was not undertaken by the Bank the probity of tender could be questioned.

4. RISK REGISTER

Both the Financial Administration and Accounting Operations risk registers address the risk of this kind of event under the Op/Information/Disclosure risk profile.

Reference	Risk Manager	Group	Definition
OPS/Information/Disclosure	Senior Manager AO, Manager AO, Senior Financial Accountant Ops	FA	Reputational – Reputational damage
OPS/Information/Disclosure	FA - Senior Managers AO, AAP, OSF and Staff Payments.	FA	Legal - breach of legislation or policy. Legal action against Bank. Fines and penalties.

5. ACTION PLAN

Action Description	Owner	Estimated Completion Date
Contact external party who received the email and request the deletion of the email and attachments, and any saved copies. Also request an email to attest that this has been done.		Complete
Withdraw the component of the tender until a later date.		Complete
Reiterate to project staff the need to correctly address emails.		Complete
Create email groups for circulation of documents related to the tender and ensure procedures are updated to reflect this as standard in future.		Complete

6. DISTRIBUTION

Assistant Governor (CS)	
Chief Financial Officer	
Senior Manager, AO	
Manager, AO	

7. SIGN OFF

Senior Manager Accounting Operations
(Acting)
Financial Administration