EXECUTIVE SUMMARY

Risk Assessment – Automatic Forwarding of Email
Data Sovereignty

October 2010

Background:

During the course of an examination of activity logs of GroupWise usage with respect to a separate matter, the Office of the Auditor General (OAG) noted an unusual amount of HRM related email being forwarded to various external service provider sites. The volume and frequency of the re-routed email resulted in a more detailed examination to determine the reasons for and possible risks associated with this activity.

Email and associated documents are proprietary corporate records of HRM and as such, are subject to a number of legislative and regulatory controls. Employees of the organization have access to information with varying degrees of sensitivity relative to their position within HRM. Employees also have the ability to exchange, store, transfer or alter records of the organization using the HRM's email system. This use should be supported with good internal processes and controls to protect the Municipality from unnecessary risks, which may result for example, from sensitive financial, personal or other information leaving the system to be stored on a permanent basis outside HRM systems, outside the province of Nova Scotia or in fact outside Canada. Once the information leaves the HRM system, the ability to monitor and control its distribution is essentially eliminated. The risks are further magnified when the business risks are considered in light of the fact that under the present system, the organization has no knowledge or ongoing monitoring of what information is in fact being forwarded and by whom and where it is ultimately being stored. An interesting and serious point is often made, "you can shut the account down, but you cannot shut the data down". Further risks are associated with the question of who has access to the various accounts where emails are being forwarded and the various methods by which these accounts are being accessed. It is entirely possible accounts are being accessed from various "internet cafes", open-user hotel machines, libraries or other locations with little control over who may also be viewing the information and what is left "behind" on various machines after use.

One function within GroupWise is the ability to create an automatic "rule" to manage one's email account. A rule can be created and set to automatically forward some or all email arriving in a HRM user account to another user account anywhere in the world. The HRM Email Acceptable Use Policy speaks to the forwarding of email to a 3rd party, requiring users to adhere to all "applicable laws and the policy." Inappropriate use may result in corrective action and/or suspension of HRM email privileges.

Scope:

We examined the GroupWise activity log of all users for the period September 1-29, 2010 and calculated the frequency of emails with a subject heading "Fwd:" being moved outside the HRM network. The HRM Email Acceptable Use Policy does allow reasonable personal use of the HRM email system. We recognized it is likely some forwarded email is personal and not a corporate record of the HRM. We did not examine the details of the referred records. Only the frequency and the location the email was forwarded to were reviewed at this time, as these are the most relevant details from a controls perspective.

Details:

Our analysis of the activity logs for the period September 1-29, 2010 identified, among other things, the following[1]:

1. A total of 625 (17.4%) of 3,600 users sent between 25% and 100% of emails received to an external 3rd party domain.
2. 159 of the 625 user accounts forwarded 100% of the email received to a 3rd party domain.
3. A cursory review of the user accounts included in the 100% threshold were those of a councillor, a police officer, a fire official, a union official and numerous line staff.
4. Approximately 45% of the outbound email was forwarded to external non-Canadian 3rd party receivers, such as @hotmail.com; @gmail.com; @yahoo.ca[2]; @live.ca[3]; @yahoo.com.

The analysis considered both the automatic and manual referral of emails to an external third party. We assumed an automatic rule was in place where 100% of all email was forwarded.

Potential Risks:

Enquiries were made of management to confirm our concerns and thoughts around the nature and degree of risk associated with this activity and what actions should be taken to reduce or

[1] Full details can be found in Attachment 1.
[2] Yahoo.ca parent company is US based
[3] Live.ca parent company is US based

mitigate the potential risks to the Municipality. The information contained in their responses to our enquiries has been included in the following points:

1. Records Management

If corporate records are being automatically forwarded to an external personal/ private e-mail account and subsequently responded to via this account, HRM's ability to manage its corporate records through these sent messages has been compromised as has the employee's likely compliance and adherence with Administrative Order #31. As well, the security of the records and the information/data contained in the records has been severely threatened as HRM no longer has security control over the records.

2. Response to FOIPOP access requests

If corporate records are being automatically forwarded to an external personal/ private e-mail account and responded to via this account, when an access to information application is received, the ability of HRM to fully respond to the request has been compromised as has the ability to confirm we have provided all responsive records.

3. Privacy Issues

If the corporate records which are being automatically forwarded to an external personal/private e-mail account contain any amount of personal information, an inappropriate disclosure of personal information has very likely occurred (a privacy breach) violating section 485 of the Municipal Government Act. Again, as noted earlier, the security of the records and the personal information/data contained in the records has been severely threatened as HRM no longer has custody or proper care and control over the records.

4. PIIDPA

The Personal Information International Disclosure Protection Act dictates HRM will ensure personal information which is in its custody or control is stored only in Canada and accessed only in Canada. Any corporate records which are automatically forwarded to an external personal/ private e-mail address hosted outside of Canada – e.g. Hotmail, Gmail, etc. and contain personal information are likely in violation of PIIDPA legislation.

Recommendations:

It is recommended HRM Administration act immediately to address the potential risks noted above and take appropriate action to eliminate these risks entirely.

Management Response:

On 12 October 2010 BPIM received, through the office of the CAO, an executive summary from the Office of the Auditor General (OAG) titled "Risk Assessment – Automatic Forwarding of Email Data Sovereignty". This memorandum represents BPIM's management response from a technology and privacy impact perspective.

The data and analysis contained in the OAG report suggests that the occurrence of forwarding of email from HRM addresses to external addresses is of concern to both the records integrity and privacy of HRM information. It is important to first understand that this risk is not uniquely assigned to email. Cover letters/memos that forward paper documentation and the forwarding of voice mails are both business practices that have been equally exposed to the same information risks for decades. Notwithstanding the long history of this information challenge, staff agrees that action must be taken to mitigate these information risks to the maximum extent possible. To that end, work was already identified in this year's business plan.

As HRM staff continues to embrace technology to improve business efficiency and as technology continues to advance at a rapid rate, BPIM staff are continually faced with the challenge of balancing the usability/productivity from our information systems with the growing necessity for information security. The major technological feature that has recently potentially increased the risk of privacy and/or records management breaches (over past practices) is the ability to automatically forward email both within and beyond the organization. This practice removes the human interface that is arguably required to ensure no negative privacy impacts result.

The OAG report indicates that 17.4% (or 625) HRM email users had forwarded between 25% and 100% of their received GroupWise email to an external email domain. This result encompasses email accounts forwarding as few as three received messages. The HRM Email Acceptable Use Policy provides that limited personal use of an HRM email account is acceptable, and in fact forwarding of personal email to an external home address is a conforming use of the email system. Staff are aware of a multitude of situations where it is completely appropriate to forward certain email messages to some of the mail domains listed in the report, which include RCMP, Government of Nova Scotia, Dalhousie, and some common third party email hosting providers used by vendors, business partners and citizens. Whether these domains are hosted in Canada or not only becomes an issue if personal information is being disclosed.

Actions Addressing "Automatic Forwarding" of Email

Staff consider the automatic forwarding of email externally without the conscious decision of an employee to be the area of greatest risk exposure to HRM. Accordingly staff conducted an analysis of a fresh data set in an effort to determine which of the users were automatically forwarding 100% of their email to an external address. Email logs were checked to determine which user accounts had immediately forwarded "HRMAll" messages to external destinations, a clear indication of an automated rule. There were 98 accounts (2.7%) participating in this practice. The majority of users engaging in the automatic forwarding practice were from Halifax Regional Library, Halifax Regional Police, and Fire Services.

Staff conducted random follow up with the individual users and members of respective management teams to determine the business reasons for their current automatic forwarding practice. Most of the users contacted indicated that 'convenience' was the primary factor in forwarding their HRM email to a home or external account. Availability of access to remote email was also a major factor, as there is a cost associated with the provision of secure ID tokens to allow such access, and it requires management approval. A number of users had technical difficulties using the remote access tools provided by HRM, and were using automatic forwarding as a work around for their issues.

With a better understanding of the scope and magnitude of the risks with automatic forwarding of email, quick action was taken by staff to:

- *inform the existing users of this practice (identified above) that it is not acceptable, completed Oct 25, 2010;*
- *direct the removal of such rules by the user, completed Oct 25, 2010;*
- *monitor and enforce compliance with the direction, full compliance achieved by Nov 15, 2010;*
- *provide alternative solutions through standard IT support channels, completed Nov 16, 2010;*
- *inform the remainder of HRM's email users of the risks associated with this practice, in particular those risks associated with potentially disclosing personal information and/ or impacting the ability to properly manage HRM records. This was completed via attached memo Nov 16, 2010.*

The above actions were completed by Nov 16, 2010. The automatic forwarding practice has been ceased within HRM and compliance monitoring is in place.

It should be noted that in the case of rules-based forwarding of email, disabling this feature in GroupWise – which would prevent any automated forwarding to external addresses – would have the detrimental effect of disabling vacation notifications, as well as a number of electronic messaging services provided to both staff and the public. This would represent a widespread

productivity hit to the organization and staff feels that the steps taken above strike the necessary information security balance required to mitigate the risk at this time. Please read the section on future technology below.

Actions Addressing "General Forwarding" of Email

The remainder of email users who 'consciously' forward emails represent a different challenge. It is generally felt that in cases where a conscious decision to forward an email either internal or external to the organization is being made, an effective strategy to deal with privacy and records management issues is through enhanced education regarding the user's individual responsibility to comply with applicable legislation.

To address this concern, BPIM will develop an education and communication program to advise email users of their responsibility for effective management of email, particularly as it relates to the forwarding of email outside the organization. The education and communication piece will focus on "good" business practises, the responsibility each employee has, the protection of information- personal and confidential, and legislative compliance. The following areas will be addressed and practical do's and don'ts (with a corresponding easy to understand explanation as to why) will be provided:

- *adding personal information to emails and protecting personal privacy*
- *treating confidential matters accordingly*
- *forwarding corporate emails to your personal account*
- *forwarding corporate emails externally for legitimate business practises.*

BPIM staff view this education and communication component as an interim measure until such time as a corporate Routine Access Policy, Privacy Policy and Email Management Policy are finalized. It is anticipated these will be completed and implemented by the second quarter of 2011/2012. It should be noted that the general lack of ICT policies, standards, and procedures was identified as a key business risk in the 2010/11 Business Plan. This situation has come about through a lack of resources; however, resourcing is being addressed through the current BPIM organizational restructuring that will see specific resources assigned to address this gap.

Future Technology

It should be noted that BPIM is currently in the early planning stages for a migration of our corporate email system from GroupWise to Microsoft Exchange, with execution tentatively commencing in late 2011. This migration will allow an opportunity to evaluate and implement additional functionality to assist in compliance/controls with FOIPOP requests, electronic discovery, internal investigations, and additional reporting capability. In the course of engaging all stakeholders, BPIM would welcome the participation of the OAG staff in the specification and selection process of additional tools which might enhance our ability to both mitigate data leakage and privacy risks, as well enhance our ability to respond to future electronic messaging challenges.

Attachment 1

Summary Data - September 1 - 29, 2010

Top 15 Domains HRM Forwarded to:

Domain	Total Outbound Messages to	Forwarded Messages to	% Forwarded to Domain	% Forwarded of Total	Likely US destination
@hotmail.com	28,204	8,401	29.8%	23.3%	x
@gmail.com	15,052	5,038	33.5%	13.9%	x
@eastlink.ca	19,454	4,785	24.6%	13.2%	
@ns.sympatico.ca	13,932	3,407	24.5%	9.4%	
@accesswave.ca	3,836	1,736	45.3%	4.8%	
@yahoo.ca	4,140	1,498	36.2%	4.1%	x
@live.ca	1,880	1,017	54.1%	2.8%	x
@rcmp-grc.gc.ca	4,594	636	13.8%	1.8%	
@bellaliant.net	1,030	580	56.3%	1.6%	
@gov.ns.ca	8,772	565	6.4%	1.6%	
@yahoo.com	2,248	547	24.3%	1.5%	x
@bell.blackberry.net	763	486	63.7%	1.3%	
@nsfs.ns.ca	471	421	89.4%	1.2%	
@dal.ca	3,147	375	11.9%	1.0%	
@staff.ednet.ns.ca	2,562	337	13.2%	0.9%	
Other Domains	106,535	6,295	5.9%	17.4%	
Totals	216,620	36,124			

Users with forwarded messages by % thresholds

Threshold	Cumulative User Count	User Count
100 % messages forwarded	159	159
75% messages forwarded	250	91
50% messages forwarded	397	147
25% messages forwarded	625	228

Users with forwarded messages (counts)

	% Outbound messages forwarded				
Outbound Message Count	100%	75%-99%	50%-74%	25%-49%	Total
>1,000	0	3	0	0	3
≥ 500	0	4	0	0	4
≥ 200	6	16	2	4	28
≥ 100	30	21	4	2	57
≥ 50	16	6	4	9	35
< 50	107	41	137	213	498
Total	159	91	147	228	625
3,600 users	4.4%	2.5%	4.1%	6.3%	17.4%

* estimated user accounts including Library and Water Commission