Data Breach Investigation
Office of the HIA Interim Advocate

NICS Group Internal Audit and Fraud Investigation Service
17 June 2020

Contents

Executive Summary

Background

1.1
On Friday 22 May 2020, the Interim Advocate's Office (IAO) issued a newsletter by email to subscribers on their mailing list. The email addresses of recipients were visible to all who received the email.

1.2
The NICS Group Internal Audit and Fraud Investigation Service was tasked by The Executive Office to carry out an independent investigation into this incident.

Findings

1.3
The investigation found that this breach occurred because the email issuing the newsletter was created by copying the email addresses from the IAO mailing list into the 'To' field of the email rather than the 'Bcc' field.

1.4
'Bcc' stands for 'blind carbon copy' and is a way of sending emails to multiple people without them knowing who else is getting the email. Any email addresses in the 'Bcc' field are not visible to anyone else receiving the email.

1.5
When issuing the newsletter, the normal process within the IAO is to copy the email addresses into the 'To' field of the email and then subsequently move them into the 'Bcc' field. However in this case, the email was unintentionally sent before this was done.

1.6
A number of recommendations have been made to prevent a reoccurrence and improve data protection / information management arrangements within the IAO.

Introduction

Background

2.1
The Head of the Civil Service tasked The Executive Office (TEO) officials to draft primary legislation predicated on the Hart Report recommendations for a statutory Commissioner for Survivors of Institutional Childhood Abuse (COSICA). Separately, officials were tasked with appointing an Interim Advocate for victims and survivors of institutional childhood abuse as a precursor to the appointment of the statutory Commissioner. The Interim Advocate was subsequently appointed by the Head of the Civil Service on 2 July 2019 and the Interim Advocate's Office (IAO) was established on 12 August 2019.

Data Breach

2.2
On Friday 22 May 2020, the IAO issued a newsletter by email to subscribers on their mailing list. The email addresses of recipients were visible to all who received the email.

2.3
The Group Internal Audit and Fraud Investigation Service (GIAFIS) was tasked by TEO to carry out an independent investigation into this incident.

Investigation Objectives

2.4
The specific objectives for the investigation were to:

- Establish the circumstances which led to the release of 251 email addresses; and
- Make recommendations to address any system weaknesses identified during the investigation.

2.5
The IAO is required to provide information regarding this incident to the Information Commissioner's Office (ICO). The information contained in this report will address some of the information required but is not, nor was it intended to be, the full report of the incident required by the ICO.

How the Data Breach Occured

Investigation Objective

3.1
To establish the circumstances which led to the release of 251 email addresses.

Findings

3.2
The IAO periodically sends a newsletter to individuals whose details are held on their mailing list (contained on a spreadsheet). When issuing the newsletter by email, the normal process within the IAO is to copy the email addresses from the mailing list, paste them into the 'To' field of the email and then subsequently move them into the 'Bcc' field.

3.3
Bcc stands for 'blind carbon copy' and is a way of sending emails to multiple people without them knowing who else is getting the email. Any email addresses in the 'Bcc' field are not visible to anyone else receiving the email.

3.4
On the afternoon of the 22 May 2020, the IAO Office Manager was preparing to send a newsletter by email. In line with normal practice, she copied the email addresses from the mailing list and pasted them into the 'To' field of the email containing the newsletter attachment.

3.5
Before moving the email addresses to the 'Bcc' field, the Office Manager was reviewing the email addresses on screen and noticed that one of the email addresses included a space which she thought was unusual. She 'minimised' the draft email so she could access the mailing list to confirm the email address. Having checked the email address, the draft email was reopened and the Office Manager continued to review the email addresses.

3.6
At this point, she started to receive a number of undeliverable messages. When the Office Manager opened one of these messages she realised that the draft email (which still contained all the email addresses in the 'To' field), had issued.

3.7
The Office Manager advised that she does not know how this happened and the only logical explanation is that she may have accidentally hit 'send' when moving between the draft email and the mailing list.

3.8
The Office Manager told us that the unsent email she was working on was open on her screen at this stage and there was another draft email within her unsent 'drafts' mailbox. Both these emails are currently showing in the Office Manager's unsent 'drafts' mailbox. The time stamp of one is the same as that of the email which issued and the second has a time stamp of six minutes later. The Office Manager has advised that she did not create these additional emails.

3.9
The unsent emails were reviewed and it is confirmed that the list of recipients, body of the email and attachment of both of these emails are identical to the one which issued.

3.10
We have explored with Digital Shared Services (DSS) the possibility that the creation of the additional emails and the unintentional sending of the email was the result of a software issue, however, there is no evidence available to determine if this was the case.

Recall Attempt

3.11
The email issued at 14:42 on 22 May 2020 to 251 recipients – 248 external and 3 internal.

3.12
A recall attempt was made at 14:44 the same day. One message, to an internal recipient, was successfully recalled. It should be noted that message recall does not work for messages sent outside the organisation.

3.13
There were 34 messages undelivered. This can happen, for example, when the email address is incorrect.

3.14
When the email was sent it included a read receipt request. This is a request for the receiving party to send a reply acknowledging that they have received the email. The recipient decides whether to provide this acknowledgement; there is no way to force this with email. There were 4 read receipts returned – 3 internal and 1 external.

Conclusion

3.15
Putting email addresses into the 'To' field and then moving them to the 'Bcc' field creates a risk that materialised in this case as the email was unintentionally sent while the email addresses were sitting in the 'To' field.

3.16
While we cannot definitively explain the creation of the additional emails and the unintentional sending of the email, irrespective of this, the root cause of this incident was the fact that the email addresses were put into the 'To' field; had the email addresses been in the 'Bcc' field when the email issued unintentionally, the data breach would not have occurred.

3.17
The only way to eliminate the risks associated with sending the same email to multiple email addresses is to create a separate email for each recipient; it is acknowledged that this may not be practicable when issuing an email to over 250 recipients. To minimise the risks when sending an email to multiple recipients whose email addresses must be kept confidential, **it is recommended** that the email addresses are input directly into the 'Bcc' field.

3.18
We note that the 'Bcc' field is not automatically shown in Outlook; this has to be manually added by the user. We will be separately recommending to DSS that the NICS email system preferences are set to automatically include the 'Bcc' field. We will also be recommending that DSS consider the potential for a software solution which will prompt the user to review and confirm before sending, that recipients have been included in the correct field (ie To / Bcc) when an email is issuing to multiple recipients.

3.19
To ensure that emails do not issue before the message and attachments are complete, **it is recommended** that the recipients' email addresses are only added once the email is ready to send.

3.20
As highlighted above, 34 messages were undelivered which suggests a problem with these email addresses. **It is recommended** that the undelivered email addresses are reviewed and the mailing list up-dated as appropriate to ensure that the information it contains is accurate.

System Weaknesses Identified

Investigation Objective

4.1
Make recommendations to address any system weaknesses identified during the investigation.

Findings

4.2
During the course of this investigation we identified a number of areas where we consider system improvements are required and these are set out in this section. However, this investigation only considered processes directly relevant to the data breach and did not include a full review of the information management arrangements in place within the IAO. Therefore, system weaknesses may exist which were not identified through this investigation. Therefore, **it is recommended** that a full review of the information management arrangements in place within the IAO is carried out.

Roles and Responsibilities

4.3
When the IAO was established it was intended to be independent from TEO and the relationship between the IAO and TEO is modelled on that of an Arms' Length Body (ALB). However, the status of the IAO appears to have created ambiguity regarding information management responsibilities, for example, in relation to information asset ownership.

4.4
It is recommended that TEO review information management responsibilities in relation to the IAO to ensure that the responsibilities of both the IAO and TEO are clearly understood and addressed.

Data Protection Officer (DPO) Role

4.5
The role of the DPO is to monitor compliance with the General Data Protection Regulation (GDPR) and inform and advise on data protection obligations. The DPO must be independent, an expert in data protection and adequately resourced.

4.6
In the two quarterly assurance statements provided to TEO for the period September 2019 – March 2020, the IAO highlighted '*no internal Data Protection Officer within this small office – referral to departmental DPO as required.*'

4.7
Contact details of the DPO are required to be included in an organisation's privacy notice. It was determined that the Office Manager would be recorded as the DPO on the IAO privacy notice as an interim measure.

4.8
There were concerns expressed (by the Senior Accountable Officer and the Office Manager) that the Office Manager may not have the skills or training for the DPO role; the intention was that once additional staff were in place, the DPO role would be revisited.

4.9
At an accountability meeting on 18 May 2020, the IAO highlighted to TEO concerns that the organisation did not have sufficient resource for an in-house DPO and asked if TEO's DPO could be used. TEO indicated that this was not possible but would look for an alternative solution.

4.10
It is recommended that the DPO role within the IAO is reviewed and a decision taken on how to ensure the role is properly fulfilled.

Policies and Procedures

4.11
We note that it was originally envisaged that the IAO would have established their policies and procedures before the commencement of the Redress Scheme. However, the legislation was enacted earlier than expected leading to an increase in the volume of queries from clients and resulting in a delay in policies and procedures being developed.

4.12
The current IAO guidance on data protection / information management is contained in their Induction Pack under the heading 'Procedures for Answering the Telephone'. This provides practical guidance on call handling and does address the issue of obtaining and recording consent for individuals' details to be placed on the IAO mailing list. However, as the only data protection / information management guidance available within the organisation, it is inadequate to assist staff in managing and protecting information, particularly in light of the personal and sensitive information which the IAO holds.

4.13
Of particular relevance to this incident is the absence of guidance on managing and reporting data breaches. Such guidance facilitates a quick, effective and orderly response to data incidents including: assessing the risks and communicating with the individuals affected, reporting to the ICO and the records and documentation to be retained. We note that the IAO used an NICS Data Breach Notification Checklist to guide their actions in reporting the breach to the ICO and notifying affected persons, however, this checklist does not provide full guidance for managing data breaches.

4.14
It is recommended that comprehensive data protection / information management policies and procedures for the IAO are developed as a matter of urgency. Procedures should include instructions on how to transmit information both electronically and in hard copy.

4.15
While we note that the IAO is an interim body and that COSICA is in the process of being established, the investment of time to develop policies and procedures for the IAO could assist in ensuring that appropriate policies and procedures are in place in advance of COSICA becoming operational.

Consent

4.16
When individuals contact the IAO by phone for the first time, they are advised that the IAO maintains a mailing list for people wanting to receive general updates. The individuals are asked to confirm consent for their details to be added to the mailing list.

4.17
GDPR requires organisations to have an effective audit trail to demonstrate how and when consent was given. For oral consent this should be a note of the date and time of the conversation and what the individual was told at the time; this should include a copy of the script used at that time.

4.18
The Office Manager reviewed the format of the IAO mailing list in April 2020 to minimise the amount of personal information contained within it. Instructions were issued to staff advising that the updated mailing list contained the details of individuals who had previously provided their consent and that no one should be added to the mailing list without them having confirmed consent.

4.19
We reviewed the guidance available to staff and the format of the previous mailing list and the current mailing list (established April 2020) and noted the following:

- The record of consent does not contain the level of detail necessary to comply with GDPR requirements. Review of a sample of entries on the mailing list identified that consent was indicated in approximately 65% of cases, however, this consent was not always explicitly stated. In a further 26% of cases, where consent was not indicated, the individuals concerned are connected to a group and consent may have been provided by the group. However, when consent is provided by a third party, they need to demonstrate that they have authority to act on behalf of the individual and this evidence must be retained.
- There are various spreadsheets containing personal information which are used for different purposes. In relation to the mailing list, the Induction Pack directs staff to a different spreadsheet to record consent.
- The Induction Pack does contain some guidance regarding obtaining consent, however, a standard

script is not used. A standard script provides wording to be used when asking for consent to ensure that all necessary information is relayed to the individual in accordance with GDPR requirements.

4.20

It is recommended that, when developing the policies and procedures as recommended at 4.14, a full review of consent arrangements is undertaken.

Training

4.21

The Senior Responsible Officer and the Officer Manager both completed 'GDPR Awareness' training in 2018 and 'Responsible for Information' training in 2019. As the IAO holds sensitive information, **it is recommended** that all individuals (regardless of their role), should on appointment to the IAO and then regularly thereafter, undertake information management training (or refresher training as appropriate).