BARNSLEY METROPOLITAN BOROUGH COUNCIL

Report of the Executive Director of Communities and ICT Manager

INFORMATION GOVERNANCE PERFORMANCE – Quarter 4 2016/17

1. Purpose of Report

1.1 To advise of BMBC's position in relation to information security breaches and cyber incidents which have been reported and investigated in quarter 4 for the financial year 2016/17. The report also provides a comparison and summary for the whole financial year 2016/17 with the previous financial year 2015/16.

2. Background

2.1 There are three reporting regimes; reporting to the Information Commissioner's Office for the most serious incidents; reporting via the information governance toolkit for adults' social care and public health most serious incidents and internal reporting and investigation. Further guidance on the reporting regimes can be found at Appendix A.

3. Overall Position for Quarter 4 2016/17 – Information Security Incidents

3.1 There have been a total of 46 incidents for Quarter 4 requiring investigation. This figure includes both actuals[1] and weaknesses[2] and third party incidents.

The table below provides a summary of incidents reported and investigated from 1st April, 2016 to 31st March, 2017 including weaknesses and including an end of year total comparison with the year 2015/16 incidents.

Management of incidents						
Quarter	**Year 2015/16**	**Q1 2016/17**	**Q2 2016/17**	**Q3 2016/17**	**Q4 2016/17**	**Total 2016/17**
Total number of incidents (including weaknesses)	**35**	**15**	**25**	**24**	**46**	**119**
Of which number of incidents reported to ICO	1	3	0	1	0	4
Of which number of incidents reported via information governance toolkit	0	0	0	0	0	0

There has been a major rise in reported incidents from the financial year 2015/16 and the previous financial year 2016/17. This can partly be attributed to the fact that

[1] Actual event – incident confirmed as a breach of Data Protection

[2] Weakness – identified as a risk to Data Protection but not a breach. These incidents are identified as a weakness as they could have caused a risk to the organisation; however the incident was contained within the Council – for example incorrect email sent internally, documents left on printer etc. There are still lessons to be learned.

awareness has been raised through policies, through SMT/BLT and through staff communications and training.

3.2 **Q4 actual incidents and weaknesses – subject to internal investigation - Directorate, Business Unit / type** (actual and weakness, excluding third party and unsubstantiated)

Business Unit	Type	Actual	Weakness	Total
Communities BU8 - Stronger, Safer & Healthier Communities	10.Unauthorised Access/Disclosure	1	0	1
Place BU4 - Economic Regeneration	4.Disclosure in Error	1	0	1
Place BU5 – Culture Housing & Regulation	10.Unauthorised Access/Disclosure	1	0	1
People BU1 - Education, Early Start & Prevention	10.Unauthorised Access/Disclosure	1	0	1
People BU1 - Education, Early Start & Prevention	4.Disclosure in Error	1	4	5
People BU1 - Education, Early Start & Prevention	11.IG Other	0	1	1
People BU2 - Adult, Assessment & Care Management	11.IG Other	0	2	2
People BU2 - Adult, Assessment & Care Management	4.Disclosure in Error	1	0	1
People BU3 - Children's Social Care & Safeguarding	11.IG Other	0	1	1
People BU3 - Children's Social Care & Safeguarding	2.Lost/Stolen Hardware	1	0	1
People BU3 - Children's Social Care & Safeguarding	4.Disclosure in Error	2	2	4
People BU3 - Children's Social Care & Safeguarding	7.Non-secure Disposal-Paperwork	0	1	1
Public Health BU10	4.Disclosure in Error	0	2	2
Human Resources, Performance & Communications BU14 - Human Resources	11.IG Other	0	2	2
Human Resources, Performance & Communications BU14 - Human Resources	4.Disclosure in Error	7	2	9
Finance, Assets & Information Services BU11	4.Disclosure in Error	0	1	1
Finance, Assets & Information Services BU13 - Finance	11.IG Other	0	2	2
Total		**16**	**20**	**36**

3.3 The highest numbers of actual incidents (12) that have occurred fall under the category 'disclosed in error'. This category covers information which has been disclosed to an incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. The main errors for Q4 are around use of e-mail. E-mails containing confidential information sent to wrong recipient / contact groups, incorrect recipients copied in, not using bcc, not encrypting / sending securely

3.4 The principles of the Data Protection Act that have been breached are as follows. Principle 7 is the breach where the ICO is likely to impose a fine and this is the one that has been most frequently been breached.

Principle 4	Personal data shall be accurate and, where necessary, kept up to date
Principle 7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

3.5 **Incidents – reported and under investigation by ICO for Q4**

No incidents have been reported to ICO in Q4, however in the financial year 2016/17 a total of 4 incidents were reported. The ICO have confirmed that they will not be taking enforcement action against the Council on these incidents. This is because of the prompt action we have taken to minimise risk, the policies, processes and procedures we have in place, the staff training we have in place and the staff actions that we take following incidents.

However, there have since been two further incidents that were reportable to ICO (April 2017). The ICO have confirmed that enforcement action will not be taken against the Council, as arrangements are in place for the Council to review its handling of personal data.

An ICO consensual audit has also been commissioned which will take place in October 2017.

3.6 **Summary of lessons learned / action taken**

Lessons / action
• The introduction of security tagged bags • Text messages not to include personal/sensitive information – email issued by Head of Service • Ensure accuracy of information and confirm that the address detail is correct prior to sending out sensitive documents • Ensure electronic databases are updated timely • Staff to pay due care and attention when sending and replying to e-mails • Risk assessment on transporting data undertaken • Be more vigilant when moving offices – secure disposal of paperwork when moving offices

3.7 **Third Party Incidents**

There have also been a total of 9 third party incidents. These range from schools, foster carers, Berneslai Homes, members of the public. These have been reported to IG but investigated by relevant parties.

3.8. Summary Information Governance Incidents

E-mail is the largest source of error in Q4. E-mails have been inappropriately sent where the recipient's address should have been carefully checked, incorrect recipients copied in, lack of security around e-mails (eg Egress), not utilising the bcc functionality. These errors have occurred both internally and externally.

The incorrect posting of documents also rate highly in the overall major sources of error.

Policies and procedures exist and training is provided to all staff throughout the Council. Every individual in the organisation has a personal responsibility to protect information. The IG Team will issue further guidance for staff around use of e-mails.

The Information Governance Board and Service Directors continue to support Information Governance with the investigation and resolution of incidents.

4. Cyber Incidents

A Cyber-related incident is anything that could (or has) compromised information assets within Cyberspace. "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."[3]

Below is a summary of the 'attempts' and 'attacks' the Council have received for the financial year 2016/17.

Action	Q1	Q2	Q3	Q4	Total
Phishing advice given	**65**	**59**	**80**	**16**	**283**
Phishing action taken	**10**	**42**	**120**	**79**	**188**
Phishing attack	**0**	**2**	**10**	**1**	**13**
Other	**18**	**9**	**22**	**4**	**53**
Total	**93**	**112**	**232**	**100**	**537**

4.1 **Definitions**

Phishing advice given - e-mail received analysed and no further actions could be taken to block further similar e-mails coming into the Council, advice given to the recipient on how to spot further phishing attempts, and what to do with the e-mail they have received

[3] Source: UK Cyber Security Strategy, 2011

Phishing action taken – e-mail received analysed and actions taken including: block further e-mails from the specific sender, get the website linked to from within the phishing e-mail removed, escalate to law enforcement agencies or escalate to e-mail subject eg Barclays Bank or Paypal.

Phishing attack – a phishing e-mail has been received and has been successful, so resolutions have been closing network accounts if details have been compromised or removing PC's from network and removing any virus, sometimes flattening PC

Other – these are requests for advice, information etc, anything security related not falling in above categories

4.2 Summary Cyber Incidents

There has been a decrease in the number of phishing e-mail calls being processed with some of this due to internal staff levels. In the first part of this next quarter we have seen a considerable increase in the number of phishing calls, this is due to catching up the backlog and marked increase in the amount of Phishing and Malicious e-mails being received.

As we are becoming more aware of the types of phishing that the Council is receiving, we are actively blocking and preventing access to more links, e-mail addresses and websites than ever before, this is part of the proactive approach that we take to IT security, with regular updates appearing in straight talk including a recent one, following on from government advice about increase risk around election time.

We have re-purchased the phishing software which now allows us to offer training to staff immediately and automatically. The functionality is enhanced and if employees click on a link or open a document inappropriately then they will be notified immediately. A small education piece will then be completed. This should further raise awareness. We see this as being the next step forwards in terms of training, with this being more focused than the general Information Security Training that has to be completed by all staff further raise awareness.

5. <u>Recommendations</u>

It is recommended that:-

- Executive Directors/Directors (where appropriate) are aware of the potential impact of information security incidents and cyber incidents on the Council and the potential for fines;
- Executive Directors/ Directors (where appropriate) are aware of information security incidents and cyber incidents in their area of responsibility and ensure full and timely reporting and investigation; ensuring lessons are learned and implemented within directorate;
- Following the recent phishing attempts and the results of the internal exercises to continue to educate staff, instigate a further internal phishing exercise and to report the results to SMT and IG Board to identify further actions
- To consider the delivery of future training and education of staff

NOTE: following the Information Security Incident Reporting Policy being revised, approved and communicated HR felt it appropriate to deliver bite-sized training to managers to raise awareness of the incident reporting policy and to deliver a strong message of the consequences of data breaches. Diane Arkwright was supported by Helen Weldon to deliver the training where awareness of employee actions has also been raised, with the aim of ensuring consistency across the Council.

Five courses were planned (which would have allowed attendance of 50-60 managers) at different times of the day, keeping them short – 45 minutes. Efforts are continuing to ensure good officer attendance at these sessions.

Appendix A

Reporting to the Information Commissioner's Office

The Information Commissioner's Office (ICO) have the authority and power to impose fines where there has been a serious breach of the Data Protection Act 1998 (DPA). The amount of the monetary penalty determined by the Commissioner cannot exceed £500,000. It must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others.

The ICO has powers to serve a monetary penalty on data controllers who fail to comply with the data protection principles. Although there is no legal obligation on data controllers to report breaches of security, ICO believe that serious breaches should be reported. To serve a monetary penalty notice for a breach of the DPA, the ICO must be satisfied that - there has been a serious contravention by the data controller, the contravention was of a kind likely to cause substantial damage or substantial distress; and either, the contravention was either deliberate; or, the data controller knew, or ought to have known that there was a risk that the contravention would occur, but failed to take reasonable steps to prevent the contravention.

Reporting via the Information Governance Toolkit

All organisations processing Health, Public Health and Adult Social Care personal data are required to use the Information Governance Toolkit Incident Reporting Tool to report level 2 IG 'serious incidents requiring investigation' to the Department of Health, ICO and other regulators. This requirement is only necessary when a certain threshold has been met[4].

Reporting and Internal investigation

If the above formal reporting requirements do not apply then BMBC still have a responsibility as a data controller to assess the risk and manage incidents appropriately ensuring that appropriate measures are put in place to mitigate repeat occurrences. Internal reporting is a valuable tool for identifying the scale of the problem, and common errors that may be eliminated through changes to systems, training or greater awareness.

BMBC's 'Information Security Incident Reporting Protocol' defines the reporting and investigation requirements. This protocol was reviewed and re-published on the Information Services intranet site in April 2016. A communication was distributed via Straight Talk.

This report outlines the information security breaches reported and investigated both internally and to the ICO and includes the data for the financial year 2015/16. Future reporting will be on a quarterly basis.

Reporting of Cyber Incidents

All organisations processing Health, Public Health and Adult Social Care personal data are required to report and investigate cyber incidents. This was a new requirement of the IG toolkit in 2015.

A cyber-related incident is anything that could (or has) compromised information assets within cyberspace. "Cyberspace is an interactive domain made up of digital networks that is

[4] **Scale factor** - number of individuals affected, **sensitivity factor** – detailed personal/confidential information at risk, harm to the individual eg distress, individual placed at risk eg physical harm, potential for media attention etc

used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."

The IG toolkit outlines the categories for cyber incidents and the requirement to report level 2 IG 'serious incidents requiring investigation' to the Department of Health, ICO and other regulators. This requirement is only necessary when a certain threshold has been met[5].

[5] **Scale factor** - number of individuals affected, **sensitivity factor** – detailed personal/confidential information at risk, harm to the individual eg distress, individual placed at risk eg physical harm, potential for media attention etc

IG

Q1 and Q2 – more that full year previous

ICO CP conference document wrong address – confirmed no fine. Immediate action taken, worker too responsibility for error, training/procedures in place

Same issues – incorrect address – meeting to take place with Mel – BS

Cyber

Rise in incidents – increased reports – though no of attacks increasing – one last week

NHS Lincolnshire, Tescos etc

Internal exercise and training – lots of negativity from staff

Separate report – or enough detail