BARNSLEY METROPOLITAN BOROUGH COUNCIL

Report of the
Executive Director of
Communities and
Head of IT
(Service Management)

INFORMATION GOVERNANCE PERFORMANCE – QUARTER 1 2017/18

1. Purpose of Report

1.1 To advise of the Council's position in relation to the number of information security breaches and cyber incidents which have been reported and investigated during Quarter 1 for the financial year 2017/18.

2. Background

2.1 Currently, 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 for security breaches and cyber. Further guidance on the reporting regimes are detailed within Appendix A.

3. Overall Position for Quarter 1 2017/18 – Information Security Incidents

3.1 There have been a total of 52 incidents reported for Quarter 1 of which 46 required further investigation, and 6 required 3rd party involvement.

Following an initial investigation, 6 were found to be unsubstantiated, 14 are undergoing further investigation and therefore subject to change.

The table below provides a summary of incidents; actuals[1] and weaknesses[2] reported and investigated between 1st April 2017 and 30th June 2017. It includes a comparison with Quarter 1 from the previous year:

QUARTER 1	2016/17	2017/18
Total number of incidents (including weaknesses)	**15**	**40**
Of which number of incidents reported to ICO	3	2
Of which number of incidents reported via information governance toolkit	0	0

There has been a significant spike in the number of reported incidents during the last two years. This can partly be attributed to the fact that awareness has been raised through policies, SMT/BLT, regular staff communication and mandatory training.

[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.

3.2 **Quarter 1: Actual incidents and weaknesses – subject to internal investigation by Directorate, Business Unit and Type** (actual and weakness, excludes third party and unsubstantiated)

PERIOD	April		May		June		Quarter 1	
BUSINESS UNIT	Actual	Weakness	Actual	Weakness	Actual	Weakness	Actual	Weakness
Communities BU7 Customer Services	0	0	0	0	0	0	0	0
Communities BU8 Stronger, Safer, Healthier Communities	0	0	0	0	0	0	0	0
Communities BU12 Information Technology	0	1	0	0	1	1	1	2
Place BU4 Economic Regeneration	0	0	0	0	0	1	0	1
Place BU5 Culture, Housing & Regulation	0	0	0	1	0	0	0	1
Place BU6 Environment & Transport	1	0	1	0	0	0	2	0
People BU1 Education, Early Start & Prevention	0	2	1	0	0	1	1	3
People BU2 Adult Social Care & Health	1	1	0	0	2	2	3	3
People BU3 Children's Social Care & Safeguarding	2	2	0	2	1	0	3	4
Public Health BU10	0	0	0	2	0	0	0	2
Core Services BU14 Human Resources	0	0	0	4	2	0	2	4
Core Services BU15 Organisation, Workforce Improvement, Communication & Marketing	0	0	0	0	0	0	0	0
Core Services BU18 Health & Safety	0	0	0	0	0	0	0	0
Core Services BU11 Assets	0	2	0	2	0	0	0	4
Core Services BU13 Finance	1	0	0	1	1	0	2	1
Core Services BU17 Legal Service	0	0	0	0	0	0	0	0
Core Services BU19 Governance & Members Support	0	0	0	0	1	0	1	0
TOTAL	**5**	**8**	**2**	**12**	**8**	**5**	**15**	**25**

	Quarter 1	
Incident Category	Actual	Weakness
1. Lost in Transit	0	0
2. Lost or Stolen Hardware	3	2
3. Lost or Stolen Paperwork	0	1
4. Disclosed in Error	10	14
6. Non-secure Disposal - Hardware	0	0
7. Non-secure Disposal - Paperwork	0	0
8. Technical Security Failing	0	2
10. Unauthorised Access/Disclosure	0	0
11. Other	2	6

3.3 The highest numbers of actual incidents (10) 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 Q1 are around e-mails being sent to wrong recipient / contact groups, incorrect recipients copied in, not using bcc, not encrypting / sending insecurely, letters being sent to previous/last known address of the Service User due to databases not being updated in a timely manner, checking process not followed prior to sending out/signing off documentation to be posted out.

3.4 The principles of the Data Protection Act that have been breached are as follows.

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

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.

3.5 **Incidents – reported and investigated by ICO for Quarter 1**

In total, 2 incidents have been reported to ICO during Quarter 1 (discussed and reported in the Quarter 4 report). ICO have confirmed that enforcement action will not be taken against the Council.

The number of reported incidents to date has prompted an ICO consensual audit which will take place between 17th – 19th October 2017.

A number of officers within the Council will be interviewed by ICO auditors over the three days, where specifically Records Management, Training & Awareness and Freedom of Information Requests will be reviewed and recommendations for improvement being suggested during January 2018.

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

Lessons / action
• 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 • Be more vigilant when transporting paperwork – undertake risk assessment

3.7 **Third Party Incidents**

There have been a total of 6 incidents involving third parties; these range from schools, application providers and other local authorities. Each incident has been reported to Information Governance and investigated by relevant parties.

3.8. **Summary Information Governance Incidents**

E-mail is the greatest source of incidents recorded within Quarter 1, in particular where they have been inappropriately sent. Often where the recipient's address should have been carefully checked, incorrect recipients copied in, lack of security around e-mails (e.g. not using the Egress solution), not utilising the bcc functionality. These errors have occurred both internally and externally.

The incorrect postal activities with letters and documents also rate highly in the overall categories of error.

The policies and procedures exist and training is provided to all staff throughout the Council at minimum on an annual basis. Every individual within the organisation has a personal responsibility to protect person information.

The Information Governance Board and Service Directors across Directorates continue to support the Information Governance team with the investigation and resolution of incidents. However, it is important to stress that completed forms must be submitted within 10 working days to the Information Governance team as this is breached regularly by Investigating Officers.

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]

The table below is a summary of the 'attempts' and 'attacks' the Council have received:

	2016/17			2017	
Action	**Q2**	**Q3**	**Q4**	**Q1**	**Total**
Phishing advice given	**59**	**80**	**16**	**8**	**163**
Phishing action taken	**42**	**120**	**79**	**120**	**361**
Phishing attack	**2**	**10**	**1**	**6**	**19**
Other	**9**	**22**	**4**	**10**	**45**
Total	**112**	**232**	**100**	**144**	**588**

[3] Source: UK Cyber Security Strategy, 2011

The table below, includes a comparison with Quarter 1 from the previous year:

Action	Q1 16/17	Q1 17/18	DIFFERENCE
Phishing advice given	**65**	**8**	**-57**
Phishing action taken	**10**	**120**	**+110**
Phishing attack	**0**	**6**	**+6**
Other	**18**	**10**	**-8**
Total	**93**	**144**	**+51**

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.

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 e.g. 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 an increase in the number of phishing e-mails being received throughout the Council both year on year and Quarter 4 2016/17 compared with Quarter 1 2017/18. This is following increased education across the Council and an increased threat globally.

The Council appear to be the target of specific campaigns such as the recent malicious invoice campaign, whereby Council e-mail addresses are being spoofed to make the e-mails appear more genuine to the receiver. Corporate Communications have sent an all user e-mail and will follow up with a Straight Talk article. Information Governance and Security are intending to regularly run articles in Straight Talk and the newly launched Intranet facility to raise awareness across the Council.

The Security Team have recently used phishing campaigns intended for IT Services and Elected Members. This was an idea suggested during a National Cyber Security Conference where experts suggest targeting specific professional groups, to increase the learning across organisations.

5. Recommendations

It is recommended that:

- Executive Directors/Service Directors (where appropriate) are aware of the potential impact of information security incidents and cyber incidents on the Council and the potential for ICO fines;
- Executive Directors/Service 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 the directorate;
- Following the recent phishing attempts and the results of the internal campaigns to educate staff, instigate a further internal phishing exercise and report the results to SMT and the Information Governance Board to identify further actions; and
- 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 colleagues felt it appropriate to deliver bite-sized training to managers and raise awareness to deliver a strong message of the consequences of data breaches. Diane Arkwright was supported by Helen Weldon to deliver the sessions 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 to 45 minutes maximum. Unfortunately, these sessions were poorly attended. At the point of writing this report 14 managers attended a session.

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 met4.

Reporting and Internal investigation

If the above formal reporting requirements do not apply then the Council 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.

The Council'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 e.g. distress, individual placed at risk e.g. 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 e.g. distress, individual placed at risk e.g. physical harm, potential for media attention etc.