REPORT OF A BREACH OF THE CODE OF PRACTICE FOR STATISTICS

1. Core Information

Title and link to statistical output	Cyber Security Breaches Survey 2019: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019
Name of producer organisation	Department for Digital, Culture, Media & Sport (DCMS)
Name and contact details of person dealing with report	Jackie Orme jackie.orme@culture.gov.uk 020 7211 2257
Link to published statement about the breach (if relevant)	Not relevant
Date of breach report	29th March 2019

2. Circumstances of breach

Relevant principle(s) and practice(s)	The relevant practices are T3.3 and T3.4, part of the principle of orderly release (T3) within the trustworthiness pillar: T3.3.Access to statistics before their public release should be limited to those involved in the production of the statistics and the preparation of the release, and for quality assurance and operational purposes. Accurate records of those who have access before they are finalised should be maintained. T3.4 The circulation of statistics in their final form ahead of their publication should be restricted to eligible recipients, in line with the rules and principles on pre-release access set out in legislation for the UK and devolved administrations. The details of those granted access should be recorded, together with clear justifications for access. No indication of the statistics should be made public and the statistics should not be given to any other party without prior permission for access. The list of recipients should be reviewed regularly and kept to a minimum.
Date of occurrence of breach	26th March 2019

A breach occurred late in the evening of Tuesday 26th March concerning a publication on cyber security breaches that was due to be published on Wednesday 3rd April 2019.

An email was sent very late (22:37) on 26th March by a senior analyst based in the cyber securities team, describing some of the results of some additional data analysis done by the contractor carrying out the survey. The email described the findings of the additional analysis, relating to estimated total numbers and total costs of breaches, and set these in the wider context of the survey findings. DCMS is not

planning to publish the additional analysis, as the sample sizes are relatively small and margins of error very wide for the estimates.

The email was copied to three people who are in the cyber securities policy team but not on the production list, one of whom was on leave all week.

3. Impact of the breach

Some of the high-level findings of the survey were made available to two people who are not on the production list for this statistics release.

This is not likely to have any further impact either within the department or externally, as the two individuals not on the production list have deleted the emails and are aware that the statistics were sent to them in error.

4. Corrective actions (taken or planned) to prevent re-occurrence

The Head of Profession for Statistics at DCMS was alerted to this potential breach on 27th March.

She discussed with statisticians in her team and one of them sent an email to everyone on the email chain alerting them to the breach, asking them not to continue the email conversation and asking the two people not on the production list to delete the emails containing the information disclosed in error.

Those two individuals have confirmed that they have deleted the emails and DCMS has put arrangements in place to prevent the third person from opening the emails (and that individual has subsequently confirmed that she did not open the emails and has now deleted them).

The analyst who sent the email has recognised his mistake in copying in colleagues not on the production list and has had a conversation with his line manager to remind him of the need to adhere to the code of practice for statistics.

In addition, a 'lessons learnt' review is planned for later in April, which will include discussion about to manage processes to prevent any re-occurrence of a breach.