SLIDE 16

Advice to give Data Controllers in the event of a breach

First we will look through some general advice and then we will talk through some specific advice you could provide in relation to cyber and S170 incidents.

Remedial action

The first section you looked at, remedial action, relates to steps the organisation can take in order to contain the breach, recover the personal data or mitigate the impact of a breach.

- Have hard copy documents been returned or destroyed, or have they been able to recall any emails.
- Have any incorrect recipient confirmed that the data has been deleted
- If a device is lost or stolen, have they been able to remotely wipe the device?
- If data has been lost, are they able to reconstruct the data from other sources available to them. If data has been altered, has it now been corrected.
- Has any support been provided to affected individuals? Particularly if they have identified any harm or risk of harm.
- Notifying other authorities like the police or safeguarding bodies, again this may help to mitigate any detriment or harm to affected individuals.
- It is important that with any breach the data controller investigates the root cause. This should enable them to identify what went wrong. For example, can they interview staff or conduct audit logs. This should enable them to identify areas of improvement and

potentially implement additional measures in order to prevent a reoccurrence.

Recurrence prevention

This isn't an exhaustive list, but some of the most common advice you may provide to controllers in order to prevent a breach from happening again includes:

- Reviewing their policies/procedures to ensure they are fit for purpose and whether any improvements can be made.
- Introducing secondary checks where necessary
- Turning off autofill as this may help to prevent incorrect recipients from being auto populated.
- Reviewing access controls on the system and the permissions set on documents to ensure personal data is not exposed to anyone who does not require access.
- Naming conventions on documents and reviewing where these are stored. This could help staff to clearly identify documents to prevent incorrect versions from being selected, e.g. one which is redacted compared to the original.
- Sending information password protected or encrypted could help prevent access to data if this is shared with an incorrect recipient.
- Review the physical security of documents or devices to prevent theft or access to information.
- One of the most important things to consider is staff training. This would include data protection training but also guidance provided to staff regarding system use and the processes they should be following. It is no good having all the technical security in place if staff are not aware on how to set permissions or securely password protect documents.

[Trainer 1]

SLIDE 17

Some specific advice you may provide to controllers in relation to cyber and section 170 incidents may include: .

- Conducting a force sign out on any accounts, this should help to ensure that a bad actor no longer has access

- Changing passwords: both on any affected accounts. Also, controllers should encourage staff not to use default passwords. They should also limit the number of failed login attempts for any accounts as this may help to keep accounts secure
- Removing any rules which have been set up
- Multifactor authentication can make the login process more resistant to phishing. These include two-factor authentication/multi-factor authentication, password managers, and alternative login mechanisms such as biometrics
- Secure Wi-Fi: do not allow untrusted devices to connect to your network and do not use work devices on untrusted networks outside of your office.
- A well configured firewall can stop breaches happening before they get deep into your network.
- Having up to date anti-virus or anti-malware products regularly scanning networks can allow organisations to prevent or detect threats.
- Having data-backed up can help to prevent any permanent loss of data. In addition, backups should not be permanently visible to the rest of the network and at least one of your backups should be off site. Don't leave backup drives attended and lock them away when not in use. Also, make sure you know what data is being stored in the cloud.
- Ensure that data can only be accessed by authorised users by encrypting it.
- Data controllers should consider carrying out training to help users identify phishing emails (such as using simulations) and training to encourage them users to report any suspected phishing emails they come across. Encouraging a culture of reporting phishing attempts will allow data controllers to take steps to review the technical measures they have in place and improve awareness amongst staff.
- Filtering services – send emails to spam/junk folders. Blocking services – block emails to ensure they don't reach the user. Data controllers can set up rules to suit their organisation's needs. Techniques for filtering include IP addresses, domain names, white/black listing etc.

S170

- Reviewing access controls on the system. Are staff only able to access what is necessary? Is certain information restricted?
- Having clear policies in place with staff to ensure that this outlines how they should handle data.

- Reviewing their staff contracts. These should set out the requirements for the organisation, and what staff can and cannot do with personal data. They could include clauses within contracts to outline what employees should do when leaving the organisation and that data should not be taken. This will add weight to a case if information is misused.
- Educating staff is also important. It could be that although the access was inappropriate it may not have been intentional or malicious, e.g. if someone has sent work to their personal address in order to finish work from home. Organisations should ensure staff understand what is appropriate and not can help prevent these types of incidents
- Their exit processes, for example, restricting access when an employee hands in their notice. They can also consider if it might be necessary to monitor the use of a certain employee's system use. They should also ensure that they revoke access to data when an employee leave the organisation.
- The organisation can consider legal action to ensure the recovery of information issuing things like a cease-and-desist letter to individuals to stop them using the information or to get confirmation of deletion.
- As mentioned above, controllers can take their own action through the courts for any contractual breach.

(Any questions?)