SLAUGHTER AND MAY/

November 2025

BEYOND CYBER – BEWARE OF HUMAN ERROR AND PROCESS PITFALLS

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 142 (November 2025)

High-profile cyber-attacks have dominated the headlines this year, whether that be those against Marks and Spencer, the Co-op or Jaguar Land Rover (JLR). These major cyber-attacks cause significant disruption and financial losses to businesses, with some analysts projecting the potential negative impact on JLR's revenues to be £50 million per week during the enforced shut down. However, the majority of data breaches do not involve a third- party threat actor, with non-cyber breaches consistently making up the vast majority of data breaches notified to the Information Commissioner's Office (ICO) each year since 2019.

The highest profile recent example of a non-cyber data breach was the accidental disclosure of personal data from the Afghanistan Relocations and Assistance programme by the Ministry of Defence (MoD) in 2022 which hit the headlines this summer. The potential consequences to the individuals were hugely significant, and the Government had to set up a new secret (and costly) relocation scheme for those on the leaked list.

The risk of these non-cyber data breaches arising can often be overlooked given the understandable, and correct, focus by businesses on taking steps to prevent and mitigate cyber risk. However, these non-cyber breaches can often cause the most tangible risk of harm to individuals and, as we have seen, can still result in regulatory action and/or litigation. Whilst human error in one shape or form is often the cause of these, and can never be completely eradicated, there are steps organisations can take to limit the risks of errors arising, and to minimise the impact when such human errors do occur.

Organisations would therefore do well not to overlook the measures they can take to reduce non- cyber causes of data breaches. This briefing distils recent learnings from case law, enforcement activity and regulatory guidance, as well as from matters in which we are involved, to highlight practical steps that improve day to day data governance and compliance.

Misdirected communications

Misdirected communications, whether via post or email, is a common challenge for all organisations, and is one that is all too often the result of human error. In reality, it will not be possible to completely eradicate such misdirections, and there is no common threshold as to the level of misdirections that should be accepted as part of business risk – after all, this depends on the nature of the personal data included in the communication in question. For example, a misdirected marketing email will have far less harmful implications for the affected individual than their medical details being shared. It is therefore important for an organisation to assess the implications for each of its different categories of its communications and then put in place appropriate measures to reflect that risk.

Importance of data accuracy

In the recent Court of Appeal case Farley & Ors v Paymaster (1836) Limited t/a Equiniti, Equiniti, as pension administrator, accidentally posted over 400 annual benefit statements (ABS) to incorrect addresses. Whilst this case is important in relation to the ability to bring mass data privacy claims (see our blogpost), it also provides useful learnings for ensuring that postal correspondence is correctly addressed, and on the mitigations to have in place if the communication is then still misdirected.

In this case, the addresses were provided by Sussex Police service to Equiniti, and then uploaded in two locations within Equiniti's database, in accordance with its process. Individuals moving house is obviously not uncommon, and so it is important to have processes in place to ensure that address data is accurate. In this case, Sussex Police provided updated details to Equiniti which were then entered, in the same way and in accordance with its process into Equiniti's systems.

However, when Equiniti prepared and printed the ABS, following what is referred to in the judgement as a computer "flaw" or "error of some kind", it was the original addresses that were printed on the recipients' letters rather than the updated ones.

This was not therefore a straightforward case of human error in using the wrong address. If there was any human error in this case, it would have been at an earlier stage, being in the setup of the IT system that allowed the old addresses to be kept, and, presumably, the address to be uploaded in two different locations within the relevant database used. Indeed, the use of old addresses was only possible of course due to them being retained, and then being accessible by the system used to generate the information for the ABS.

Looking at this incident in the round, both in terms of steps they had in place and steps that could have helped, and other matters in which we have been involved, other organisations should:

- Ensure there is clear responsibility and a process for receiving updated address information when this is to be provided by another party. There will always been a time lag between someone changing addresses and an organisation being notified, so consider what is the appropriate regularity for receiving updates from the third party to avoid receiving daily updates, but so as to receive them sufficiently promptly.
- Put in place regular proactive address verification prompts and/or run periodic address integrity checks. Whilst it would not have helped in this case, if there is for instance a material annual mailing as with ABS, it would be prudent to proactively prompt individuals to update their information a suitable period ahead of such a mailing.
- Ensure there is only one record per customer across the business (i.e. a single source of truth for data), as data sprawl creates greater risk.
- Review the rationale for retaining previous contact information and reassess the period for such retention.
- Ensure that where historic contact information is held for a period, that access to this is limited to those people and systems that strictly need it, to avoid the inadvertent use of old address data as was the case here.

Private and confidential markings make a difference

In Farley, the ABS took the form of a letter headed "Private and Confidential", with the scheme member's name and the postal address being visible in the envelope window. There was then a return address printed on the envelope.

When considering whether the pleaded fears (of misuse of the personal data) could be characterised as "well-founded" as opposed to being based on a "purely hypothetical risk" or similar, the Court in Farley concluded that anyone receiving one of these envelopes would see at a glance that it was a private communication, of an expressly confidential nature, which had been sent to the right person but the wrong address" and the "overwhelming majority of people do not open such correspondence but return it (as happened in more than 100 cases here) or keep it, or throw it away" and so "the chances of such a letter being opened are remote".

Some key learnings here are:

- Use private and confidential marking prominently on the envelope, or so that it is visible through the address window.
- Using window envelopes avoids the risk of letters and addressed envelopes being mismatched, but it is then prudent to ensure that there is sufficient white space around the name and address of the intended recipient so that any movement of the letter within the envelope doesn't lead to inadvertent visibility of additional personal data through the window.
- If non-window envelopes are used, check a sample of the filled envelopes to check that they contain the correct letter, and no additional letters, as we have known mail runs to accidentally include the wrong letter or indeed more than one letter in an envelope.
- Include a return address on the envelope.

Avoiding and mitigating the impact of misdirected emails

With emails, it is all too easy to send information to the incorrect person, or group of people, or to attach incorrect documents. To mitigate this:

- Mandate the use of secure file transfer or portals rather than email for sensitive data. Where this is not possible, require documents to be password protected and the password shared by another means such as text or WhatsApp. For internal emails, attach links to access-controlled documents rather than attaching copies.
- Prevent use of autocomplete of email address in mail applications, or if its usage is allowed, remind people to regularly remove old details, such as where an individual has moved companies.

- Use technical solutions to sense check email addresses that have been inserted to look for anomalies based on past patterns of recipients.
- Where possible, pseudonymise any personal data so the impact of misdirection is minimised. In Case C-413/23 P EDPS v SRB, the Court of Justice of the European Union held that if a third party receives pseudonymised data but it does not have the reasonable means to re-identity any individuals, the data will not be personal data in the hands of that third party (although it remains personal data in the hands of transferor).

Avoid accidental oversharing

As mentioned above, the risks of sharing data were highlighted this summer when it was revealed that a spreadsheet containing highly sensitive personal details of over 18,000 individuals who were part of the Afghanistan Relocations and Assistance programme was accidentally disclosed by the MoD.

This followed on from a similar set of circumstances in 2023 when the Police Service of Northern Ireland posted a spreadsheet on a public facing website in response to a Freedom of Information Act (FOIA) request, resulting in a £750,000 fine from the ICO. And earlier this year, the ICO reprimanded London Borough of Hammersmith and Fulham after it exposed, for over two years, a spreadsheet in response to a FOIA request containing 35 hidden workbooks and the personal data of employees, ex-employees and agency staff and also children's sensitive data.

All three of these data breaches arose because the controller had a genuine need to share certain information, but human error led to the accidental disclosure of additional personal data. In response, the ICO published new guidance on disclosing documents to the public securely. Whilst this was intended for public sector bodies responding to FOIA requests, it has useful learnings for all organisations on how to avoid data being inadvertently (over)shared. We have highlighted some of these below together with learnings from incidents on which we have advised:

- Convert documents to a more appropriate format. Data can appear hidden in documents such as text which has been formatted to appear invisible (such as white text on a white background) or where tabs or columns on a spreadsheet have been "hidden". Converting the document into a simpler format, such as from an Excel spreadsheet to a .csv can reveal this hidden data making it easier to review. Metadata from emails can also be removed by saving them as a .txt file.
- Check that there are no links included in the document to be disclosed. Documents containing links to other files will retain a copy of that linked document once shared, which the ICO said left open the risk of sharing more than initially intended.
- Use appropriate tools to redact data to ensure it cannot be retroactively unredacted once shared. For instance, whilst a black box over text may appear to have redacted the information, in some cases that box can simply be dragged to the side to reveal the information underneath. The ICO recommends that where access to redaction software is not available, going old school and physically redacting a hardcopy and then scanning it for electronic sharing can ensure no trace of the redacted information remains.
- Consider who in the organisation needs the ability to send or upload attachments, or attachments of certain types, and restrict, through policies and technical measures, the ability of others to do so.
- Provide clear guidance to employees on how to safely share data, including for instance, the need to scrub spreadsheets of hidden tabs, pivot caches, comments, named ranges, and metadata. Remind them at suitable intervals and include this in mandatory annual data privacy training.
- Mandate a four eyes (or more) approach depending on the risk in different situation so that there are more lines of defence to human error.

The perils of data being misfiled

One topic that is frequently arising in practice at present is the ability of AI to surface information from an organisation's systems that should not have been accessible to the person using the AI. This is therefore an increasing cause of data breaches within an organisation. The AI is not the problem here, it is just exacerbating an existing issue, i.e. data being misfiled or not having the correct security classification applied to it. Organisations, whether or not rolling out AI, should therefore consider the following steps:

- Reassess internal policies on data / document classification to ensure that they are clear and reflect real life examples to help guide people. For instance, documents on salary reimbursements between group companies may appear to be Business as Usual to the accounts team, but they will, by their nature, contain salary data of employees.

- Good data deletion policies can assist, as if data is deleted it cannot be inadvertently surfaced. However, if it has been misfiled, this brings its own risks of information being deleted without the correct authorisation, which, in itself, is a data breach.
- Implement and publicise a safe way for colleagues to report that they have access to a document that they should not have access to, without fear of reprisal.

Conclusion: fundamentals first, especially in an AI-enabled world

The cases, enforcement actions and guidance discussed above underscore a simple truth: most harmful incidents arise from well-known, preventable weaknesses. The ICO was clear in its 2024 review that it "want[s] organisations to learn from the mistakes of others by understanding what common security control failures led to breaches". Fines will almost certainly be unavoidable if organisations have not implemented the mitigating controls and preventative measures the ICO has called out in past enforcement action.

That lesson matters even more as AI becomes pervasive across business processes. Any basic error or security failing carries an amplified risk with AI, both in terms of the likelihood of an issue arising and the resulting harm to individuals. In practice, this means doubling down on the fundamentals and doing the ordinary things well.

CONTACT

REBECCA COUSIN
HEAD OF PRIVACY, SENIOR CONSULTANT
T: 020 7090 4738
E: Rebecca.Cousin@slaughterandmay.com

CINDY KNOTT
HEAD OF DATA PRIVACY KNOWLEDGE
T: 020 7090 5168
E: cindy.knott@slaughterandmay.com