

ICO confirms the number one cause of a data breach is simple human error!

At the end of October 2020, the Information Commissioners Office (ICO) released their latest security incident report, and its findings should really come as no surprise given the challenges business's and their employees have faced because of the ongoing COVID-19 pandemic.

The data covers the period April to June 2020, relates to cyber incidents (e.g., ransomware/phishing scams) and non cyber incidents (e.g., information emailed/faxed/posted to the wrong person) and reports across 11 sectors.

As we move into a very uncertain 2021 it is crucial that Businesses continue to adapt to the new and predominantly digital world. The findings of this report should act as a warning that having access to the technology to protect outbound email data is no longer a "nice to have" but a vital necessity given that the number one cause of data breaches is noted as simple human error - An email and/or attachments being sent to the wrong person.

Indeed, if we consider the whole period since the European Union's General Data Protection Regulation (GDPR) we have seen the number of data security incidents reported to the ICO increase by 75 per cent. Yet a huge 88 per cent of them were not the result of deliberate cyber incidents, but rather human error. More than a third were security incidents relating to data being emailed, posted, or faxed to an incorrect recipient by mistake.

It is fair to mention here that this is something we can all relate to and indeed have all no doubt done at some point in our careers. The risks, however, are rising dramatically as email traffic increases and the pandemic takes its toll on our workloads and wellbeing. Now, more than ever, employees need to be supported in their roles, with the appropriate technology to hand, to enable them to meet both client and compliance expectations.

From April to June 2020 the ICO tells us that there were 266 incidents reported where data was inadvertently emailed to the wrong recipient. If we consider the fear of recrimination amongst employees, we must assume that the true figures may be much higher with many incidents going unreported, a real concern for Compliance Managers and Business owners alike.

Regular training around good cyber security practices is now crucial, a point highlighted in the report's findings that there were 185 incidents attributed to phishing scams. This puts a business at a 44% higher risk of a mis directed email causing a data breach than a phishing email. This seems astonishing given the prolific phishing scams that have surfaced during the COVID-19 pandemic and must surely be attributed to the well published warnings and training that has been delivered to prevent this type of breach.

Maillock, from our cyber security partner Beyond Encryption is a secure email system that can support employees and protect against these potentially very damaging business risks. Encryption is used to prevent email interception as a result of cybercrime, and identity verification processes ensure that the data is only made available to your intended recipient.

Maillock also fully integrates with Unipass identity services.

Maillock is the recommended secure email solution for members of The Right Mortgage Network and is available at a special rate of £8.50 (+VAT) per user/ per month.

[Register Here for your 14-day free Maillock trial](#)