Importance of print security in organisations

Law, Security

In a recent survey undertaken by Gartner, it is estimated that the average business spends between 1% and 3% of their total revenue on print. This is a huge cost to businesses and organisations. With document security and data being critical in businesses today, it is vital that all office devices are audited and included in your cyber security plans. When auditing laptops, smartphones, tablets and desktop computers it is very easy to overlook multi-function devices and photocopiers. But did you know that 70% of organisations have been the victim of inadvertent data breaches through security holes in their print device infrastructure*? Even more worryingly, IT teams still don’t take the print infrastructure of organisations seriously when it comes to cyber security.

Why should organisations secure their printers?

Average end users do not have much if any reason to worry about how much printing they do, and print security is often one of the furthest things from their minds. Even if documents are tagged as confidential or sensitive, end users often don’t consider the potential implications of a data breach. With printing being such a vulnerable path to data breaches, potential ways in which they can happen include situations where hardware used to print is used without the intention of the end user. Sleep settings and auto standby modes often cause users to print and produce extra copies of documents which are not required. This means that sensitive and confidential papers can often end up being discarded without being destroyed or shredded and end up in the public domain.

Another way that printing can be insecure is via authorised internal users printing confidential information to printers that are shared. This widens the risk of documents being picked up by mistake by another user who sent the previous job to the printer, especially if the printer is situated far from where the original user is based. Multiple copies of print jobs can also be left unattended or forgotten about in out trays if users send jobs to a printer but request it again from a device that is closer to their desk.

Where confidential information is produced regularly, priority should be placed on those departments to ensure they have good practice when it comes to ensuring the security of documents that contains sensitive information. If this information gets into the hands of a disgruntled employee for example, this can be particularly dangerous.

What steps can organisations take towards print security?

Determining what level of security is required for print devices is the first step to take, and careful consideration needs to be undertaken of how to achieve this. Naturally, priority should be given to those departments that regularly produce and print confidential documents, as they are likely to be more prone to data breaches. Education about data breaches and how easily they can occur, even in printing devices, is key. Users should be given facts and figures on the cost of data breaches, as well as what the financial impact of breaches on organisations will be. Although this is seen as the responsibility of the IT department, the more education there is around the impact of data breaches as a result of insecure printing activity to all users,

the better. To learn more about the latest print technology, please contact our expert team today.* – research from Quocirca.