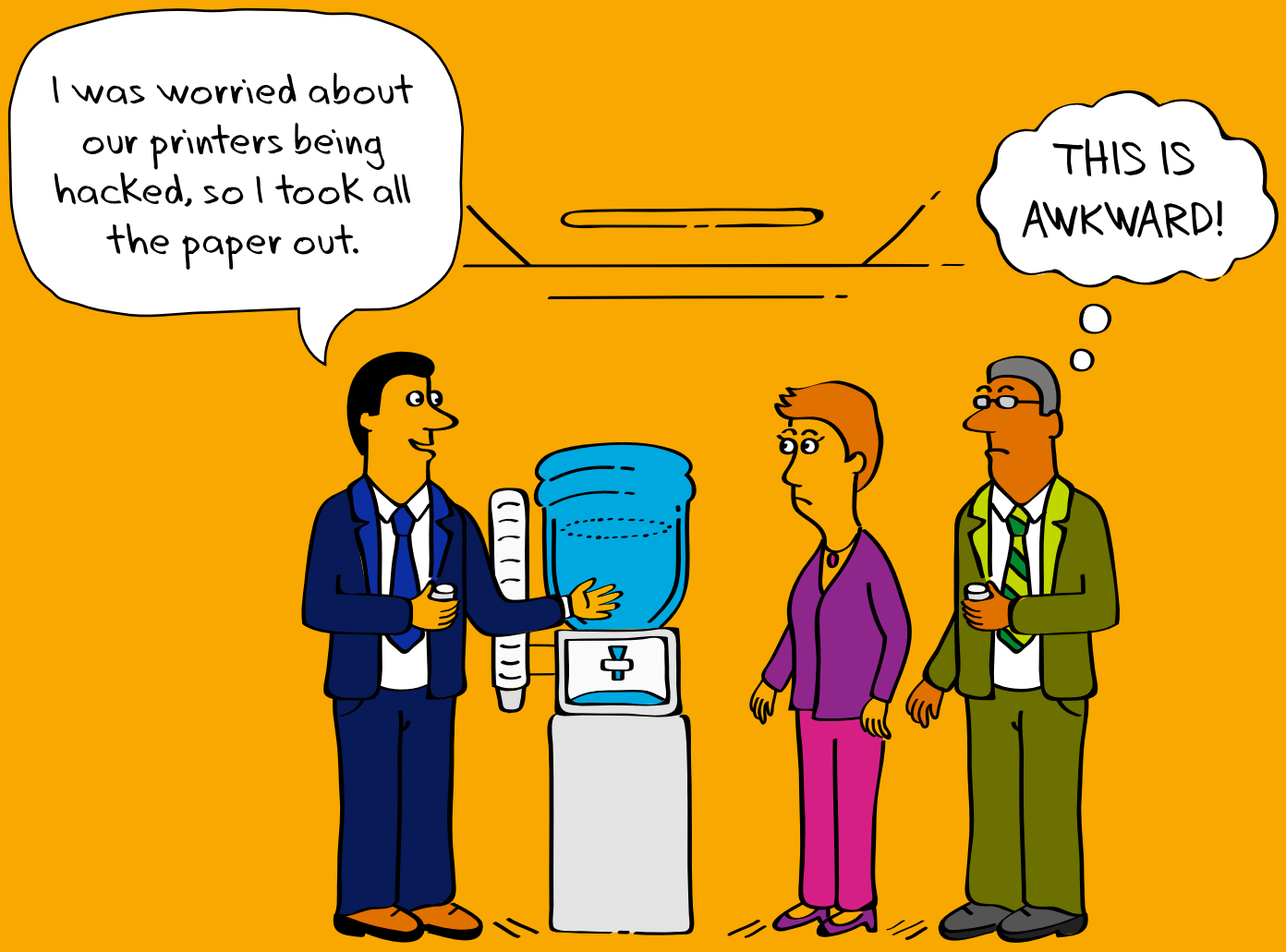
brother
at your side

SMBs: Ignore Print Security at your Peril

brother.co.uk/socially-awkward



Who wants to talk about print security?

We want you to avoid those printer conversations that can seem a little awkward. So, let's discuss printer security and GDPR here and now. GDPR (General Data Protection Regulation) is the EU's latest legislation on data protection and privacy for citizens. As an SMB, it's crucial you comply with GDPR. Fall foul, and you're looking at fines of €20 million (£17.6 million) or 4% of your global turnover — whichever value is greater.

This whitepaper aims to make it easy for SMBs to include print security in their GDPR measures. It'll highlight the areas of risk and offer security solutions that don't require enterprise-sized resourcing.

GDPR for SMBs

GDPR touches all areas of a company's operations, including printing. But printing can be a blind spot for SMBs, as a recent survey found out.[1] The survey, which targeted SMBs and large enterprises in Europe, revealed that:

- Just 22% of all businesses surveyed were completely assured their print infrastructure was secure
- Only 24% of SMBs said they were likely to include print security in their GDPR measures

Where to focus

The evolution of Multi-Function Printers (MFPs) has been great for SMBs. For instance, **modern-day MFPs** provide print, copy, scanning and faxing services through fixed-line or wireless connectivity to multiple persons across multiple devices.

However, because MFPs are essentially network-connected devices with processing power and inbuilt storage, they could be a route into your network for hackers and a threat to your data security.

For example, it's not hard to imagine a trespasser walking into your office, going straight up to a printer and taking away confidential documents. Or going up to a printer, inserting a USB stick and launching a malware attack on the network.

Wi-Fi is another potential area of weakness. Staff love your printers' Wi-Fi connectivity, but if your printers are attached to an unsecured Wi-Fi network, hackers can access the

device and data without even entering the building. And don't be fooled by having an office on the 10th floor. Unsecured networks can be attacked however high up they are.

Your MFP most likely has security functions built in to help fend off any attacks across your network. But if those security functions are still governed by their default passwords, hackers can easily get past them.

It's vital that you secure your network and properly activate the security settings on your printer to ensure unauthorised people don't gain physical access to your documents.

The good news

For SMBs, GDPR compliance doesn't automatically mean a large cost outlay.

Brother's SMB laser printer range has a host of embedded security features that can be deployed to 'serve and protect' a business from GDPR's heavyweight penalties. And while every SMB should have suitable firewalls and anti-virus software running to protect against hackers, these printers are far from defenceless.

With a pull-printing solution, such as **Brother's Secure Print+**, you can provide employees with PINs or key cards that ensure print jobs can only be released once the user is at the device. This will prevent sensitive documents being left unattended.

If you want to take your security to the next level, look no further than **Brother's Secure Function Lock** feature. Administrators can limit users' access to device functions, such as access to settings, so even if their credentials fall into the wrong hands, interlopers are still barred from tampering with the device.

Make sure you change the default passwords on your printers. Plus, frequently update firmware and drivers. And if/when you do decide to upgrade your printers, choose devices that use secure protocols such as TLS (the successor to SSL) and SFTP, while encrypting all data.

You don't have to go it alone

The risks are clear, and eliminating the risks should be clear enough too. But there's the time factor. As an SMB, you already have a long list of things to do, and GDPR and secure printing feels like just another, albeit vital, one.

At Brother, we offer Managed Print Services (MPS) so you stay focused on your business, while we manage your printer environment, including its security. As part

of our **Brother MPS solution**, our personnel will identify unprotected devices or those that might already be infected by malware. Furthermore, as part of our MPS offering, we'll advise you on ways to increase printer security by, for example, standardising brands and models. It's a strategy that has proved to be worthwhile.

A Quocirca report found that:

- While 67% of those operating a multivendor fleet reported at least one data loss, this dropped to 41% for those that were operating a standardised fleet
- Companies operating a standardised fleet are 26% less likely to suffer data loss[2]

Conclusion

GDPR cannot be overlooked. Just as importantly, print security must be a top GDPR measure. It's true that when addressing security issues, SMBs don't always give printers the attention they deserve. But there are multiple ways your printer fleet can be an entry point for criminals.

Fortunately, it's also true that **Brother SMB laser printers** come with features such as **Secure Print+**, and **Secure Function Lock** to help you protect your data and stay on the right side of GDPR legislation.

All you need to decide is whether to address your printer security alone or with a managed print service. But what you don't need to do is strike up a conversation with a friend discussing your print security nightmare, because Brother can provide you will all the answers. **For further information visit brother.co.uk/socially-awkward**

1 Quocirca Managed Print Services Landscape, 2017. European survey results of 180 midmarket (500-999 employees) and large (1000+ employees) organisations in UK, France and Germany using a managed print service.

2 Quocirca, Print Security: An Imperative in the IoT Era, January 2017