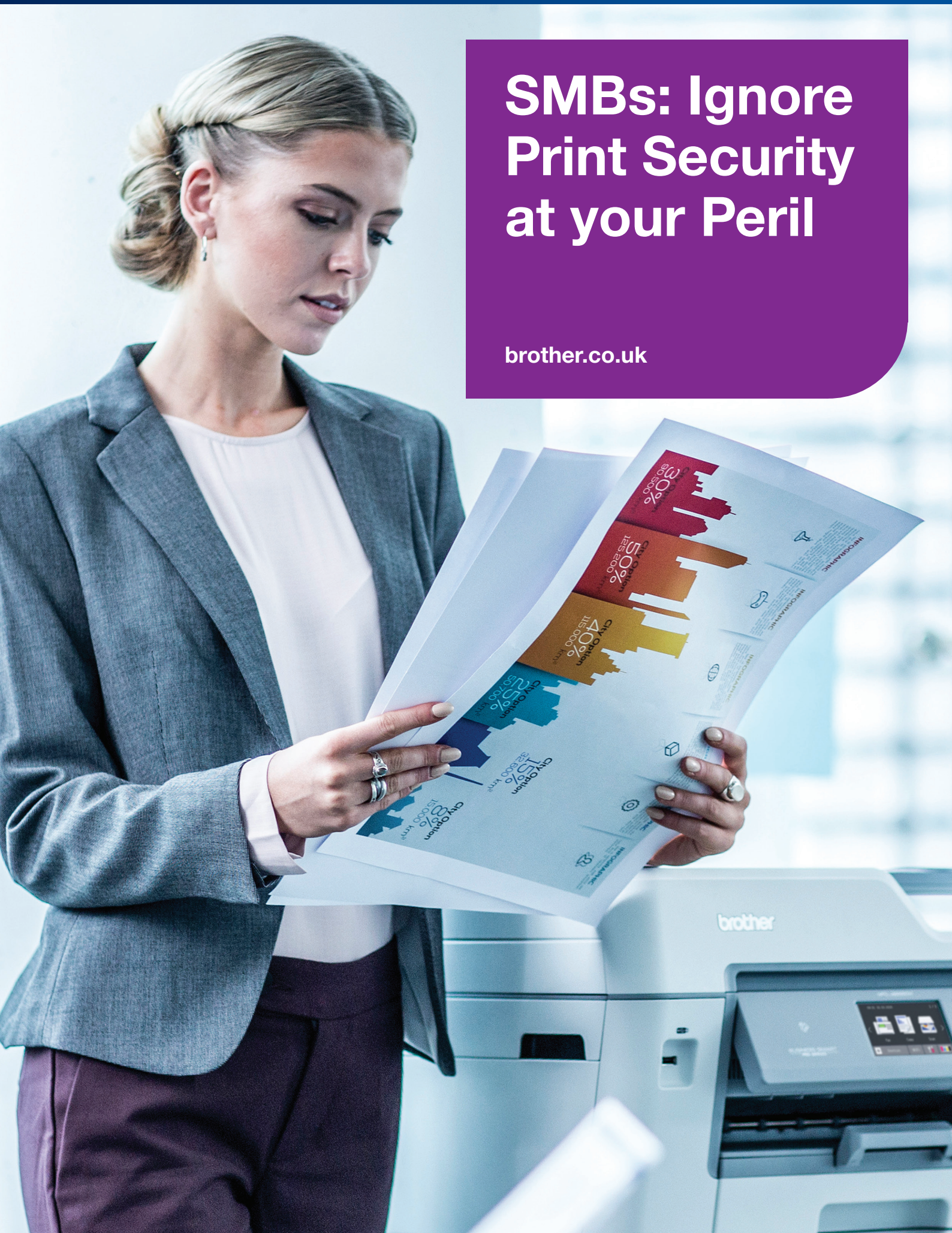
brother
at your side

SMBs: Ignore Print Security at your Peril

brother.co.uk



5,026,547 – that is the number of data records that are lost or stolen every single day.[1] Yet despite the escalating number of breaches, many still believe that large enterprises are the only businesses at risk. This belief isn't just incorrect; it's potentially catastrophic. As a result, too few SMBs have adequate security procedures and systems in place, and notably are overlooking a key element in their infrastructure – their print fleet.

This whitepaper aims to help remedy this situation. It'll highlight the ways your print environment is putting you at risk and offer up security solutions that don't require enterprise level resources.

5,026,547 data records are lost or stolen every single day.

How bad is the problem?

The UK government's 2017 Cyber Security Breaches Report picked up on the security malaise amongst SMBs. It noted that business attitudes to cyber-security distinctly correlated to company size. The smaller a firm was the less likely they were to see cyber-security as a high priority and implement formal policies related to it. For those lacking policies and governance, their reasoning why was revealing. Overwhelmingly they claimed "to be too small or insignificant to have such things in place." However, a quick look at the breaches suffered and this reasoning rapidly falls apart; 52% of small businesses and 66% of medium businesses suffered a breach within the year.

However, that's just the start of it. 74% of breaches were only uncovered after six months or more,[2] meaning a huge amount of breaches go completely undetected every year. And considering that a U.S. National Cyber Security Alliance report found that 60% of small businesses went out of business within six months of a breach[3], SMBs can ill afford to ignore these threats.

60% of small businesses went out of business within six months of a breach.

But is print really a concern?

Well, in 2017 an enterprising grey-hat hacker rather easily hijacked 150,000 insecure printers from a variety of businesses.[4] Fortunately, his intent was to raise awareness, but it clearly demonstrated the potential dangers that unsecured printers pose. But that wasn't just a one-off; IDC's Print Security Survey found that more than 25% of all IT security breaches involved print,[5] and when you consider the type of data that passes through your printers on a day-to-day basis, you'll quickly realise why it's vital you secure it. Your finance department might be printing an invoice one moment whilst HR print an employee contract the next. Personal data is worth big-bucks to hackers and your print environment is rife with it. IBM estimates that the cost of each lost or stolen record containing sensitive information is £98.[6]

£98 – The cost of each lost or stolen record containing sensitive information.

How is your print environment vulnerable?

Multi-Function Printers have evolved drastically over the years and are now complex network-connected devices with inbuilt storage and processing capabilities. That means that they are not only a source of valuable data but a potential route into your network. There are a number of ways in which attackers can access them, ranging from physical breaches to network intrusions and employee negligence.

Up close and personal

As isolated devices often sit in the corner of an office, printers can be the first port of call during a physical intrusion. On a simplistic level there is little to stop trespassers walking up and taking confidential documents that have been mistakenly left in the tray. However, physical attacks can get more complex. As an endpoint that is often left unprotected, intruders can launch malware onto the printer through a USB stick or USB connected device. This can either find its way onto the network or sit on the printer collecting sensitive data that passes through it.

Over the air waves

Interlopers don't necessarily have to be at a device to breach it. If your printers are attached to an unsecured wireless network, for instance your guest network, intruders could access the device without even entering the building. Don't think that being in a high-rise office will keep you safe either. Researchers in Singapore proved that with nothing more than a drone and mobile phone, they were able to detect an open wireless printer on the 30th floor, mimic it and intercept documents that were intended for the real device.[7]

Via the network

Whilst it's a far harder attack vector, hackers can breach your print devices over the internet. It's possible to search for network-connected devices with insecure network ports and gain access. One group of Russian hackers used this method to penetrate a Denmark-based company, gaining access to their network via one of its label printers. They then demanded a ransom to unlock the company's IT systems, customer information and other vital data.[8]

Now whilst each of these methods will not immediately grant the attacker direct access to your network, there are a number of things they can do to get in.

Basic network protocols like SMTP and SMNP have long been used in the management of print devices. Unfortunately, hackers can abuse these protocols if they're not properly secured or updated. They can interfere with the communication process and reroute messages, essentially enabling man-in-the-middle attacks. These attacks can then allow hackers to gather internal IP addresses, communication port information and even usernames and passwords.

What you can do to protect yourself

Whilst every company should have comprehensive security including firewalls and anti-virus software, there are a number of printer specific actions that can be taken.

To get started there a variety of simple changes that can be made. It might seem obvious, but many organisations come unstuck by simply forgetting to change the default passwords on their printers. It's also vital that you frequently update firmware and drivers. Unsurprisingly legacy devices are most at risk in this regard, so skip out on upgrading at your peril. And if you do decide to make the move to a modern, secure device, remember to properly dispose of those being replaced - printer hard drives can potentially contain sensitive information.

When it comes to securing access to your printers, there are a number of solutions on the market that can completely shut down this attack vector. With a pull-printing solution, such as Brother's Secure Print+, you can provide employees with PINs or keycards and ensure that print jobs can only be released once the user is at the device, which can prevent sensitive documents being left unattended. Depending on your company's needs, this can be applied to all printing or on a job-by-job basis. If you want to take your security to the next level, then look no further than Brother's unique Secure Function Lock feature. Administrators can limit users' access to devices, so even if their credentials fall into the wrong hands, interlopers are still barred from tampering with the devices' settings.

When deploying new devices, it's best to stick with ones that use secure protocols such as TLS (the successor to SSL) and SFTP, and encrypt all data that passes to and from your printers. To make this easier print management solutions contain protocol controls that allow you to easily disable protocols that aren't required. These solutions can also ensure that if the worst does occur, you're able to identify the breach and take remedial action before it's too late.

Overall the most effective way to easily implement these solutions is to partner with a managed print services provider. They'll deliver top-of-the-line secure devices and provide expert advice, guidance and support. To begin with they'll perform an audit of your current printer setup, where they'll be able to pinpoint unprotected devices and any anomalies within them, which could include malware infections. They can also help to reduce risk by consolidating your entire fleet. One 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.'[9] And when your legacy devices reach the end of their lifecycle, an MPS provider can safely collect and recycle them, guaranteeing your data won't go astray.

Those operating a standardised fleet are 26% less likely to suffer data loss.

Conclusion

Whilst the threats facing organisations of all sizes are greater than ever, it's no longer the case that you need the hulking security budgets and resources of an enterprise to meet them. Today's comprehensive solutions and managed print service offerings can help ensure that your defences are extended to all of your endpoints and that your print fleet continues to empower your business instead of putting it at risk.

1 http://breachlevelindex.com/

2 Sophos, Synchronized Security: Best-of-breed defense that's more coordinated than attacks, May 2017

3 https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

4 http://www.bbc.co.uk/news/technology-38879671

5 https://www.idc.com/infographics/printsecurity/ATTACHMENTS/PrintSecurityInfographic.pdf

6 IBM 2017 Cost of Data Breach Study UK, June 2017

7 https://www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/

8 https://www.itworldcanada.com/wp-content/uploads/2016/09/ITW-16333M-A-Guide-to-Print-Security-for-Canadian-Organizations.pdf

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