Why SMEs Need Expert Support When It Comes to Print Security

Data security used to be a concern reserved for large businesses. Small and medium size enterprises (SME) owners were more likely to worry about their information security as consumers than in their business context. But as the digital age evolves and GDPR becomes enforced, the security threat landscape is becoming more complex, and SMEs are increasingly in the crosshairs. Nearly half of all cyber attacks target small businesses, and the losses aren't small. In fact, the average loss for every 100 compromised records is more than £20,000 – to say nothing of the damage a breach could do to your company's reputation.

Although a study by our partners Xerox showed that more than 40% of businesses still rely primarily on paper processes, most don't make print security a priority, choosing to focus instead on their desktops, laptops and servers – if there's a security plan in place at all, and hackers know this.

Many businesses don't appreciate the seriousness of the risk. Today's new multifunction printers are going beyond print, scan, fax and copy to truly help SMEs increase productivity and improve the way they work. But left unsecured, any intelligent networked device can act as an open door to the network if left unprotected. Reports of MFPs (Multi-Function Printers) being hacked through open ports is becoming more common and demonstrates the need to ensure devices are protected from unauthorized access.

Another surprising risk comes from your people themselves. From BYOD (Bring your own Device) to paper left in the printer tray to simple mistakes made by a busy employee, team members, though well intentioned, can be a serious security risk, one that is likely to fly under your radar. Fortunately, there are several ways to minimize the risks to your business, and they are surprisingly easy to manage.

Assess the Threat

If you're a larger organization with a diverse printer fleet, you should strongly consider enlisting the help of a Document Management Services (DMS) provider to assess device, fleet and enterprise document security. An assessment will locate the existing points of vulnerability and help you put a customised security plan in place that will take into account all factors, from user access to what to do with the device and its stored data when it's time to upgrade.

Integrate Device Protection

Hard drive encryption is standard on most MFPs, along with data overwrite features. Data overwriting can help you safely upgrade to a new device when the time comes, without worrying what information is leaving with it. A sound, comprehensive device protection service ensures that your MFPs do not provide open access to the network, and that all open ports are closed as needed.

Lastly, enabling automatic firmware and software updates means you never have to worry about installing patches or making other manual adjustments. You'll always have the most up to date protection, without any interruption to your workflows, or assigning additional responsibilities to your team members.

Secure Your network

There are a few ways to make your MFP more secure. The most common way is to encrypt print jobs to make it safe for sensitive documents to be printed via a wired or wireless network. Current MFPs use a comprehensive set of capabilities to prevent malicious attacks and unauthorized access. Those devices enabled with Embedded Control technology which uses application whitelisting technology to protect its devices from corrupt software and malware.

Regain Control

Few business owners restrict print access because most don't realize the threat posed by unrestricted printing. While your team members will likely never put your business at risk deliberately, mistakes like leaving critical data in a printer tray can easily lead to a breach – not to mention the print costs that add up when people print documents they don't need. PIN and pull printing enable print jobs to be saved electronically on the device, or on an external server, until the authorized user is ready to print them. The user provides a PIN code or other authentication method such as a swipe card, or fingerprint to release the print once they've arrived at the printer. No more wasted paper, and no more unsecured information sitting in the printer tray. Access controls can also ensure that only authorized users can access your MFP's functionalities, an important feature when you're using a printer with app technology, or one that holds sensitive information on its hard drive.

Monitor Your Devices Now and Into the Future

The more devices and employees you have, the more complicated the task of understanding what is being printed, scanned and copied where and by whom. A knowledgeable Data Management Software (DMS) partner can integrate print management tools that will allow them to monitor and track the usage of every MFP in your organization, giving you valuable feedback like which devices are being used, how, and by whom. This is an important piece of the puzzle as it not only protects the security of your devices and the information they store; it can ultimately lead to reduced costs and a more effective document management system. Most company's print security is an overlooked risk and an under-appreciated benefit. By entrusting a DMS provider to build an integrated approach to print security, you can protect your most valuable asset, your data, in a way that is hassle and headache free.

Green Office Technology Ltd
The Old Piggery
Kinwarton House, Alcester,
Warwickshire, B49 6HA
03333 208 343