



YOUR PRINTER HAS A MEMORY

The forgotten computer
in the corner

IS IT PART OF YOUR
CYBERSECURITY PLAN?



EXECUTIVE SUMMARY

Executive Summary

The multifunction printer in an SME is often treated as a piece of office furniture. Modern devices are better understood as networked computers that print, copy, scan, email, authenticate users and, depending on the model and configuration, temporarily or persistently store job data.

That does not mean every printer is silently keeping a complete archive of everything the business has handled. Storage, retention, encryption and erase functions differ by device. The practical risk begins when nobody knows what the device can store, who can administer it, where scans are sent or what happens to its data when it leaves the premises.

The management message: A printer should appear in the same asset register, access review, update process and disposal procedure as other networked business technology.

A useful first review should answer five questions:

1. Who has administrator access and are default credentials still active?
2. Is the device firmware supported and kept current?
3. Which scan, email, cloud and shared-folder destinations are configured?
4. Does the device contain internal storage, and how is that storage protected?
5. What verified sanitisation process applies before return, resale, repair or disposal?

REPORT INDEX

Contents

Section	Page
Executive Summary	1
Main Article	3
1 A printer is part of the network	3
2 What may remain on the device	3
3 Where everyday workflows create exposure	4
4 The risks do not end at the printer	4
5 POPIA changes the consequence, not the basic control	4
6 Secure printing is a workflow, not a tick box	4
7 The highest-risk moment may be when the device leaves	5
The 15 Minute Printer Security Check	6
8 Questions to ask before signing or renewing a contract	6
Closing Perspective	7

MAIN ARTICLE

The Forgotten Computer in the Corner

Why your office printer belongs in your cybersecurity plan

Imagine an SME replacing a five-year-old multifunction printer at the end of a rental agreement. The machine has scanned identity documents, supplier banking confirmations, employment contracts, customer orders and payroll information. It has also been configured to send files to email addresses and shared folders.

The supplier collects it on a Friday afternoon. Nobody asks whether it contains internal storage, whether the address book has been cleared, whether administrator credentials were changed or whether a sanitisation certificate will be issued. The business has completed an equipment swap, but not necessarily a secure technology handover.

1 A printer is part of the network

A modern multifunction printer may have an operating system, web administration interface, network address, user directory, email capability, applications and internal storage. It may connect to a print server, Microsoft 365 or Google Workspace, a shared network folder, a document-management platform or a vendor cloud service.

This capability is what makes the device useful. It is also why the printer should not sit outside the company's normal technology controls. A device with network access and administrative functions deserves an owner, a supported configuration and an update process.

What the device does	What management should ask
Prints and copies	Are sensitive jobs released only when the authorised user is present?
Scans to email	Which sender account and destinations are configured, and who can change them?
Scans to folders or cloud services	Are access rights still appropriate and are failed transfers visible?
Stores job or address-book data	What is stored, for how long, and is it encrypted or erased?
Provides a web administration page	Who can access it and are default or shared passwords still in use?

2 What may remain on the device

The answer depends on the model. Some devices use limited volatile memory; others have hard drives, solid-state storage or embedded flash memory. Stored information may include temporary print or scan job images, saved jobs, fax information, address books, user details, settings and audit records.

It is therefore inaccurate to claim that every printer keeps every document forever. It is equally unsafe to assume that switching a machine off, deleting an address-book entry or restoring visible settings has removed all data. The administrator must check the manufacturer's documentation for the exact model and configuration.

Practical rule: Do not guess whether a device stores information. Record its model, storage configuration, encryption status and available erase functions while the machine is still under your control.

3 Where everyday workflows create exposure

Most printer risk is not dramatic. It comes from ordinary convenience being left unmanaged.

Uncollected printouts. Payroll reports, disciplinary records, quotations and customer information may remain in the output tray.

Shared scan destinations. A general “accounts” folder or mailbox may be accessible to more people than the person scanning realises.

Old address-book entries. Documents may be sent to former employees, obsolete email addresses or incorrectly named contacts.

Open administration pages. A device that can be administered from the business network may expose settings if passwords are weak, shared or unchanged.

Personal email workarounds. Employees may route scans through private accounts when the approved process is slow or unreliable.

Uncontrolled USB use. Removable media can create another path for moving sensitive information in or out of the business.

4 The risks do not end at the printer

A scan normally moves through several components: the printer, the network, an email service or shared folder, and the recipient's device. A secure printer cannot correct an over-permissioned folder, a compromised mailbox or a recipient list that has not been maintained. Conversely, strong cloud security does not correct a device that still uses a default administrator password.

Responsibility should therefore be divided clearly. The office manager may own the device list and physical handling rules. The IT provider may manage network placement, credentials, firmware and logs. The print provider may configure device-specific security features and perform or certify sanitisation. The business remains responsible for ensuring that the complete process is defined and evidenced.

5 POPIA changes the consequence, not the basic control

The Protection of Personal Information Act requires responsible parties to use appropriate, reasonable technical and organisational measures to protect personal information. The Information Regulator's current guidance also states that security compromises must be reported through its eServices process and that an operator must notify the responsible party when it experiences a relevant compromise.

An unsecured printer is not automatically proof that a reportable security compromise has occurred. The concern is whether personal information has been lost, accessed, altered, destroyed or exposed without authority. If that happens through printing, scanning, stored device data or a connected workflow, describing the equipment as “only a printer” does not remove the business's responsibilities.

This report provides operational guidance, not legal advice. A suspected compromise should be escalated promptly to the organisation's Information Officer and appropriate legal or privacy adviser.

6 Secure printing is a workflow, not a tick box

Secure release printing can hold a job until the user authenticates at the device using a PIN, card or approved sign-in method. This reduces the chance of sensitive papers being collected by the wrong person or left unattended. It only works if the feature is configured, users understand it and exceptions are controlled.

Other controls may include device encryption, secure erase of temporary job files, signed firmware, disabled unused protocols, network segmentation, access logging and automatic deletion of retained jobs. Availability varies by model and may depend on licences, accessories, software or configuration. Buyers should ask for the required control to be demonstrated rather than accepting a general statement that the device is “secure.”

7 The highest-risk moment may be when the device leaves

Repair, replacement, return and disposal are often treated as logistics. From an information-security perspective, they are changes of custody. The business should know who collected the device, its serial number, what storage it contained, which sanitisation method was used and what evidence was retained.

The correct method depends on the storage technology, information sensitivity and manufacturer capabilities. A factory reset may remove settings without providing the same assurance as media sanitisation. Where storage cannot be reliably cleared, contractual arrangements should address retention, destruction or removal of the storage component.

Handover question	Evidence to retain
Which exact device left the site?	Asset number, serial number, model and collection date
Who had custody?	Collector identity and signed handover record
What storage was fitted?	Configuration record or service report
How was data sanitised?	Method, date, responsible person and certificate where available
Were connections removed?	Confirmation that accounts, address books, apps and destinations were cleared

Contract point

The agreement should say who owns or controls storage media, who may access it during a repair, what happens if a device is replaced with a loan unit, and what evidence will be provided when data is cleared. A vague promise to “reset the machine” is not the same as a device-specific sanitisation commitment.

The same control should apply when a technician removes a drive or replaces a controller board. The SME should know whether the part leaves the premises, how it is protected in transit and whether the service provider will notify the business if personal information may have been exposed.

PRACTICAL TOOL

The 15 Minute Printer Security Check

Use this check with the person responsible for the printer and the person responsible for IT. A “no” or “unknown” answer is a prompt for investigation, not proof that a breach has occurred.

Check	Yes / No / Unknown	Action owner
The printer appears in the current asset register.		
A named person owns its business and security configuration.		
The administrator password is unique and controlled.		
Unused network services and features are disabled.		
Firmware support and update responsibility are confirmed.		
Scan-to-email and folder destinations have been reviewed.		
Former employees and obsolete contacts are removed.		
Sensitive print jobs use an appropriate release method.		
Internal storage and encryption status are documented.		
A verified exit and sanitisation process is written into the contract.		

Acceptance rule: The device is not treated as reviewed until every “unknown” has an owner and due date, and any high-risk access or disposal issue has an agreed corrective action.

8 Questions to ask before signing or renewing a contract

1. Does this model contain a hard drive, solid-state drive, flash storage or removable storage?
2. Which security functions are standard, and which require extra licences or accessories?
3. Who is responsible for firmware updates and how will completion be evidenced?
4. Can unused ports, protocols, cloud connectors and local applications be disabled?
5. How are administrator accounts created, transferred and removed?
6. What happens to stored data during repair, loan-device replacement and end-of-contract collection?
7. Will the supplier provide a device-specific sanitisation or destruction record?
8. Who is notified if the provider, as an operator, becomes aware of a security compromise?

CLOSING PERSPECTIVE

Do Not Let Familiarity Hide the Risk

The office printer is familiar, shared and usually reliable. That is precisely why it can escape scrutiny. People notice a new server or cloud platform. They seldom stop to ask who administers the printer beside reception or what happens to the machine after the lease ends.

The answer is not to make printing difficult or to buy every available security feature. It is to place the device inside the company's normal control environment: record it, assign responsibility, restrict access, keep it supported, review its workflows and manage its departure.

For most SMEs, the first improvement costs little. Walk to the device with the office manager and IT provider. Identify the model, open the configuration record, review the scan destinations and ask what proof will exist when the machine is eventually removed. If those questions cannot be answered, the printer is already telling management where the next control improvement should begin.

Educational boundary: Device capabilities and erase methods differ. Confirm all settings against the manufacturer's documentation for the exact model and obtain specialist advice where sensitive information or a suspected compromise is involved.