



CYBERSECURITY | CONNECTED DEVICES | PRINT | VOIP | CCTV

SPECIAL REPORT

The Office Devices Your Cybersecurity Policy Forgot

Why printers, phone systems, routers and cameras belong inside the security perimeter

Practical guide for South African SMEs

A business-focused report for owners, office managers, finance managers and IT managers who need to bring multifunction printers, hosted PBX, routers, Wi-Fi, CCTV and access control into the same security review as laptops and email.

Prepared July 2026

Executive summary

Many SME cybersecurity policies concentrate on email, laptops, cloud accounts and staff awareness. That is necessary, but incomplete. A modern multifunction printer can process and retain confidential documents. A hosted PBX can expose call routing, recordings and billing. Routers, Wi-Fi access points, CCTV and access-control systems often have remote administration portals, supplier access and firmware that requires maintenance.

The gap is usually not a lack of sophisticated security software. It is a lack of basic management: no complete asset list, no named owner, shared administrator passwords, uncertain firmware status, forgotten remote access and no controlled process when equipment is replaced or returned.

South African businesses also need to view these devices through POPIA. Scanned identity documents, employee records, call recordings, camera footage and access logs can contain personal information. POPIA requires appropriate, reasonable technical and organisational safeguards, while the Information Regulator reported 2,374 security-compromise incidents in the 2024/25 financial year, up from roughly 1,700 the year before. That number covers many different causes, not only office devices, but it is a useful reminder that ordinary controls matter. Reported compromises have continued to climb into the 2025/26 financial year, with the Regulator noting an increase of roughly 40% on the same point a year earlier.

- List every connected office device and record who owns the risk internally.
- Replace default or shared administrator credentials and use multi-factor authentication where the platform supports it.
- Track firmware, support status, enabled services and remote-access permissions.
- Separate guest access and higher-risk devices from the main business network where practical.
- Treat return, resale, replacement and disposal as data-security events, not only logistics.
- Include suppliers with remote access in contracts, access reviews and incident procedures.

What this means for management

A device should not be allowed onto the business network merely because it prints, makes calls or records video. It should have an owner, a supported configuration, controlled access and a documented retirement process.

The Office Devices Your Cybersecurity Policy Forgot

Why printers, phone systems, routers and cameras belong inside the security perimeter

An SME may have a sensible cybersecurity policy and still leave important devices outside it. The antivirus contract is current. Staff use multi-factor authentication. Backups are checked. Yet the copier has the same administrator password it had at installation, the camera app is still accessible to a former employee, and nobody knows whether the router firmware is supported.

This happens because office equipment is bought and managed by different people. Finance signs the copier agreement. An office manager deals with the phone supplier. A security company installs cameras. An internet provider supplies the router. Each system works, so each is treated as somebody else's responsibility.

The practical test

For every device connected to the network, management should be able to answer four questions: What information does it handle? Who can administer it? Who keeps it updated? What happens to the data when it leaves the business?

1 The blind spot is usually ownership, not technology

The National Cyber Security Centre describes enterprise connected devices as an expanding attack surface and warns that, after compromise, they may be used as a route into the wider corporate network. Its point is not that every camera or printer is unsafe. The risk grows when devices are internet-accessible, poorly maintained or treated as an afterthought.

For an SME, the first improvement is therefore administrative. The business needs a single register covering every connected device, irrespective of who supplied it or which budget paid for it. Without that register, routine controls become inconsistent: one supplier changes passwords, another leaves defaults in place; one device is patched, another is out of support; one remote user is removed, another remains active for years.

2 What belongs inside the security perimeter

The perimeter is broader than computers. It includes any device or service that connects to the network, stores information, provides remote access or controls another business process.

Device or service	What it may handle or control
Multifunction printers and scanners	Print jobs, scanned documents, address books, scan destinations, stored credentials and device logs.
Hosted PBX and VoIP	Call routing, extensions, voicemail, recordings, billing, mobile applications and administrator portals.
Routers, firewalls, switches and Wi-Fi	The pathways between staff, cloud systems, guests, suppliers and internet-facing services.
CCTV and video recorders	Live feeds, recordings, remote-viewing accounts, retention settings and cloud storage.
Access control and intercoms	Employee and visitor access records, mobile credentials, door schedules and remote release.
Meeting-room and smart-office equipment	Wireless displays, conferencing systems, controllers and internet-connected sensors.

Not every item needs the same level of control. A boardroom display and an MFP holding scanned payroll documents are not equivalent. The register helps management decide where the greatest exposure sits rather than applying the same checklist blindly.

3 Multifunction printers: document systems with a print function

A current MFP is a networked document system. Depending on the model and configuration, it may hold print jobs temporarily, store documents in user boxes or mailboxes, maintain address books and scan destinations, connect to email or cloud folders, run embedded applications and provide a browser-based administrator interface. These capabilities are useful, but they require deliberate security configuration and maintenance.

The most common SME weakness is not an exotic attack. It is an ordinary control left unfinished: the default administrator password was never changed; staff scan confidential documents to a shared mailbox; old user boxes remain on the device; secure-release printing is available but not used; or the equipment is collected at contract end without written confirmation that stored data and address books were removed.

A practical MFP review should cover:

- A unique administrator credential held by a named internal owner, not only by the service technician.
- Current firmware and a clear answer on who applies security updates.
- Only the network protocols and services needed for the actual workflow. Disable unused services. Where a service is required, use the more secure option where supported, such as HTTPS rather than HTTP and SNMPv3 rather than older SNMP versions.
- Encrypted connections where supported, including secure web administration and protected scan destinations.
- Secure or pull printing for payroll, HR, legal, medical and customer-identification documents.
- A documented data-erasure process before return, resale, redeployment or disposal.

Why July 2026 matters for Windows printing

From 1 July 2026, Microsoft's printer-driver ranking prefers the built-in Windows IPP class driver on Windows 11 and Windows Server 2025 and later. Windows Protected Print Mode is a separate setting that uses Windows Ready Print and removes printers that rely on third-party drivers while it is enabled. Before rollout, test printer and scanner compatibility and any advanced finishing functions. The change is a reason to review print security and compatibility, not a reason to replace every printer.

4 Hosted PBX and VoIP: protect the administrator portal as carefully as email

A hosted phone system is normally administered through an online portal. That portal can change call routing, create extensions, reset voicemail, activate mobile users and sometimes access call recordings or billing. A compromised account may create privacy, fraud and availability problems at the same time.

The NCSC's PBX guidance makes an important management point: the organisation that owns the PBX remains responsible for its security and administration, even where a supplier hosts or supports it.

Review the following controls:

- Multi-factor authentication for administrator and remote-access accounts where available.
- Named accounts rather than one shared "admin" login used by staff and suppliers.
- Restrictions on international, premium-rate and after-hours calling where the business does not need them.
- A leave process for extensions, mobile applications, voicemail, call queues and recording access.
- A retention rule for call recordings and a clear reason for keeping them.
- An incident route for unexpected call charges, routing changes, locked accounts or abnormal call patterns.

5 Routers and Wi-Fi: the equipment everything else depends on

The router, firewall, switches and Wi-Fi access points carry traffic for almost every other office system. When their passwords, firmware or remote-management settings are weak, the problem is not confined to the network cupboard.

A 2026 NIST draft aimed at non-employer firms uses routine software and firmware updates for everyday devices such as printers and routers as an example of basic cyber hygiene. The underlying management point is relevant to larger SMEs as well: updates are easily missed when nobody is clearly responsible. The internet provider may support the line but not the firewall. The IT company may support laptops but not the managed switch. The phone supplier may need network changes but have no authority to make them.

At minimum, document who manages each device, whether remote administration is enabled, when configurations were last backed up, whether the hardware remains supported and how guest Wi-Fi is separated from operational systems. Where practical, cameras, access control and guest devices should not sit on the same unrestricted network as finance systems and staff computers.

6 CCTV and access control: physical security creates digital records

CCTV and access-control systems are often installed for physical security, then excluded from cybersecurity reviews. Yet they may provide internet-accessible video, cloud accounts, mobile applications, administrator portals and detailed records of employees, customers and visitors.

Current vulnerability advisories continue to include IP cameras. In February 2026, the US Cybersecurity and Infrastructure Security Agency published an advisory covering certain TP-Link VIGI-series cameras and recommended more secure methods, such as a VPN, where remote access is required. One advisory does not mean every camera is insecure. It does show why supported firmware and controlled remote access cannot be ignored.

The management review should include:

- Who can view live footage, export recordings, change retention settings or add users.
- Whether former employees, installers or security contractors still have access.
- How long footage and access logs are retained, and why that period is proportionate.
- Whether cameras and recorders are still supported by the manufacturer and receive updates.
- Whether remote access uses a controlled account and secure connection rather than an exposed device interface.
- Whether backup power, time synchronisation and restart procedures preserve useful evidence after an outage.

7 POPIA turns device management into an accountability issue

POPIA does not prescribe a specific printer setting, camera brand or firewall model. It does require a responsible party to take appropriate, reasonable technical and organisational measures to secure the integrity and confidentiality of personal information, identify foreseeable risks, establish safeguards and keep those safeguards effective. Sections 19 to 22 are therefore directly relevant when office devices process personal information.

The practical consequences are broader than cybersecurity software:

- A copier that scans identity documents needs controlled destinations, access and retention.
- A call-recording platform needs defined users, purpose and deletion rules.
- CCTV and access-control records need limited access and a defensible retention period.
- A supplier processing personal information for the business should be governed by a written contract requiring appropriate safeguards, as contemplated by section 21.
- Where there are reasonable grounds to believe personal information was accessed or acquired by an unauthorised person, section 22 notification duties may apply.

The Information Regulator's August 2025 guidance states that security compromises must be reported regardless of the organisation's assessment of the risk level. SMEs should not wait for an incident to decide who assesses the facts, who contacts the Regulator and who communicates with affected people.

Legal and operational discipline must meet

A device register is not legal compliance by itself. It creates the evidence needed to show that the business knew what devices existed, assigned responsibility, reviewed access and acted when risks changed.

8 A six-control model that an SME can actually maintain

The aim is not to build an enterprise security programme around every office appliance. The aim is to apply six controls consistently.

Control	Practical requirement
1. Know what exists	Record the device, location, purpose, model, network connection, supplier and data handled.

Control	Practical requirement
2. Assign an owner	Name the person who approves access, confirms updates and follows up the supplier.
3. Control administration	Use unique credentials, MFA where available, named supplier accounts and prompt leaver removal.
4. Maintain support	Track firmware, vulnerabilities, configuration backups, warranties and end-of-support dates.
5. Limit exposure	Disable unused services, restrict remote access and separate guest or higher-risk devices where practical.
6. Retire safely	Export needed records, remove accounts, erase stored data and obtain evidence before equipment leaves.

A small business can implement these controls gradually. Start with devices that hold sensitive information, provide remote access or could interrupt trading if compromised. A ten-year-old meeting-room display is not necessarily the first priority. An unsupported router, shared PBX administrator account or internet-facing camera may be.

9 Questions to ask suppliers before renewal or installation

Security should be part of the commercial discussion, not an appendix raised after installation. Ask for plain answers and record them in the decision file.

Review area	Question management should record
Ownership	Who is responsible for security configuration, updates and access reviews after installation?
Administrator access	Will the business receive its own administrator account? Are supplier accounts named and time-limited?
MFA and authentication	Which portals support MFA, single sign-on or role-based access?
Updates and support	How are firmware updates identified and applied? When does the device or platform reach end of support?
Remote access	What remote-access method is used, who approves it and can the business review access logs?
Data handling	What information is stored locally or in the cloud, where is it hosted and how long is it retained?
Incident support	Who must be contacted after suspicious access, and what logs or evidence can the supplier provide?
Exit and disposal	How are accounts, recordings, address books, disks and configuration data removed at contract end?

10 When something looks wrong: act without destroying the evidence

Warning signs may include unexpected call charges, unknown administrator accounts, camera settings that changed without approval, new scan destinations, a device repeatedly going offline, unexplained configuration resets or remote-access alerts.

The first response should be controlled:

- Record what was observed, when it was observed and which accounts or devices appear affected. Capture screenshots and available logs before they are overwritten.
- Contact the responsible internal owner and the appropriate IT, telecoms, print or security provider through a known contact route, not through contact details supplied in a suspicious message.
- Contain or isolate the affected device with specialist guidance where possible. Avoid unnecessary reboots, resets or configuration changes that may destroy useful evidence.
- Change relevant credentials from a trusted device after the available evidence has been captured. Check related systems where passwords or administrator access may have been reused.
- Assess whether personal information may have been accessed or acquired, then follow the business's POPIA incident and notification process without waiting for a full technical investigation to finish.
- Keep a dated record of decisions, actions, supplier instructions and evidence retained. This is important for technical recovery, insurance, law enforcement and regulatory reporting.

11 Where AI can help, and where it should not

AI can assist with preparation, not accountability. A business can use an approved AI tool to organise an exported asset list, compare supplier answers, identify missing fields in a device register or draft questions for a technical review. Security platforms may also use machine learning to prioritise unusual activity.

Do not paste passwords, private network configurations, raw camera logs, call recordings or personal information into an unapproved public AI service. The output must also be checked by a responsible person. AI cannot confirm that a device is safely configured merely because a spreadsheet looks complete.

Useful AI touchpoint

Export a non-sensitive list of device names, models, owners, support dates and last-review dates. Use an approved AI tool to flag missing owners, expired support and overdue reviews. Then verify every suggested action against the actual device and supplier documentation.

12 Conclusion: bring ordinary office devices into ordinary governance

The business does not need to treat every printer, phone or camera as a crisis. It does need to stop treating connected devices as invisible infrastructure.

A proportionate approach is enough: know what exists, assign ownership, control administrator access, maintain supported firmware, limit unnecessary exposure and remove data safely when the equipment leaves. Those controls reduce security risk, improve supplier accountability and make POPIA responsibilities easier to manage.

The strongest cybersecurity policy is not the one with the longest list of threats. It is the one that still works when the device sits in the print room, above the reception desk or inside the network cabinet.

Final takeaway

If a device connects to the network, handles business information or can be administered remotely, it belongs in the cybersecurity review. Its product category does not exempt it from management responsibility.

Connected office device security register

Complete one line for each printer, PBX platform, router, Wi-Fi controller, camera recorder, access-control system and other connected office device.

Device / location	Purpose and data handled	Internal owner / supplier	Admin and remote access	Firmware / support	Risk, action and due date

How to use the register

Start with devices that provide remote access, store personal information or would interrupt trading if unavailable. Mark each item Green, Amber or Red in the final column. Green means controlled and current. Amber means working but with a gap or unclear owner. Red means unsupported, exposed, repeatedly failing or without accountable access control.

A practical 30-day review

The objective is visibility and ownership, not a rushed replacement programme.

Timing	Action	Accountable role
Days 1-5	List connected office devices and supplier portals. Photograph model and serial labels where records are incomplete.	Office manager / IT owner
Days 6-10	Confirm internal owners, administrator accounts, MFA, supplier access and former-user removal.	Management and suppliers
Days 11-15	Record firmware, support status, enabled remote access, retention settings and configuration backups.	IT / telecoms / print / security providers
Days 16-20	Prioritise Red items: default credentials, unsupported equipment, exposed remote access, unknown owners and missing disposal controls.	Responsible manager
Days 21-25	Test one incident route: suspicious camera login, PBX fraud alert or unauthorised scan destination.	Management and support providers
Days 26-30	Approve actions, budgets and review dates. Add the register to quarterly technology and contract reviews.	Owner / finance / IT

Management decision record

Record what was found, which risks were accepted, which actions were approved, who owns each action and when the register will be reviewed again. A security review that produces no owner or date is only a discussion.

Important note: This report provides practical management guidance. It is not legal advice and does not replace a technical security assessment where a material exposure or incident is suspected.