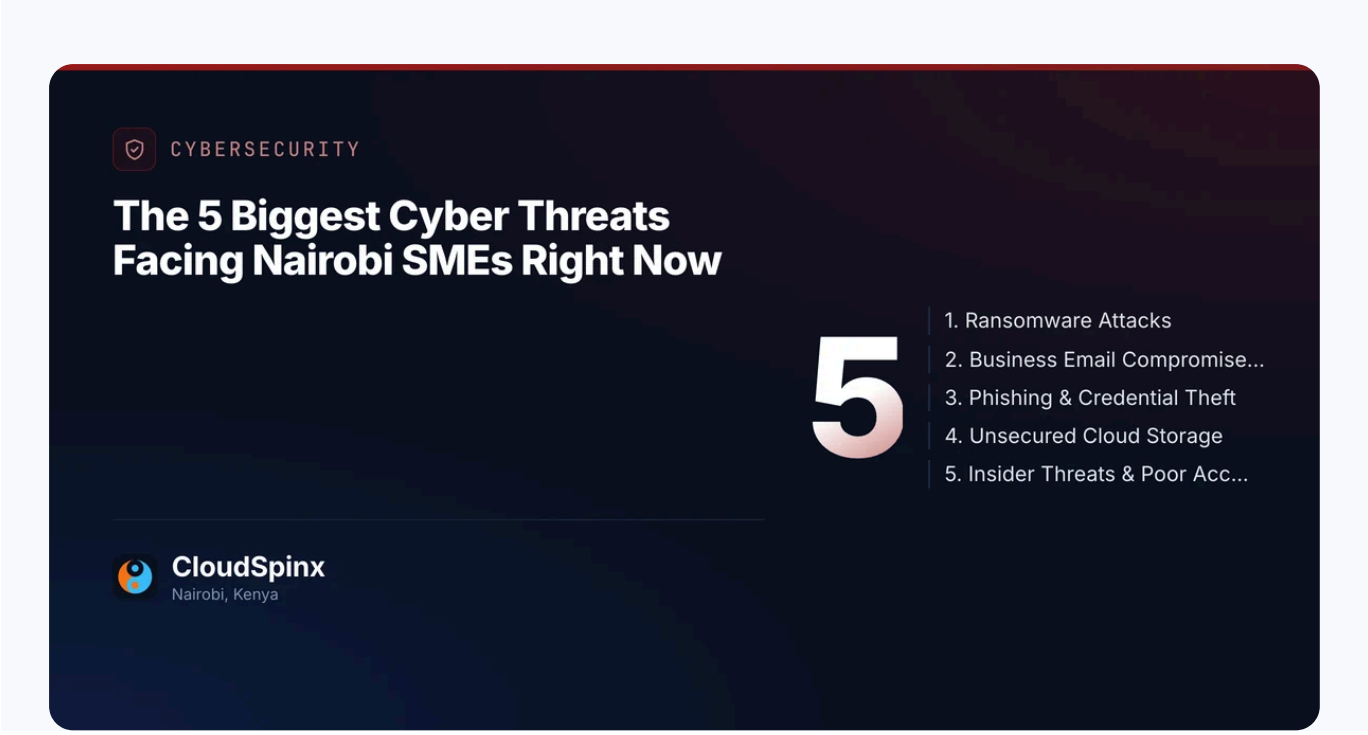

CloudSpinx Kenya cloudspinx.co.ke

Kenya's digital economy is growing fast, and so is cybercrime targeting it. The Communications Authority of Kenya reported over 1 billion cyber threats in 2024 alone, with SMEs increasingly in the crosshairs.

The good news: most of these attacks are preventable with the right controls. The bad news: most Nairobi businesses don't have those controls in place.

Here are the five most dangerous cyber threats hitting East African SMEs right now, and what you can do about each one.

1. Ransomware Attacks

Ransomware encrypts your files and demands payment (usually in cryptocurrency) to unlock them. In Kenya, average ransom demands have grown to KES 500,000 to 5 million for SMEs. Even if you pay, there's no guarantee you'll get your data back.

Why it's growing in Kenya: More businesses moving operations online, combined with limited security investment, makes SMEs attractive targets. Attackers

specifically search for businesses using outdated Windows systems or unpatched software.

What to do:

- Maintain regular, tested backups stored offline or in a separate cloud account
- Keep all software and operating systems patched and updated
- Deploy endpoint detection and response (EDR) software on all devices
- Segment your network so ransomware can't spread to all systems

2. Business Email Compromise (BEC)

BEC is one of the most financially damaging attacks facing Kenyan businesses. An attacker gains access to a business email account (or spoofs one convincingly) and impersonates a senior executive, requesting urgent fund transfers.

Kenyan businesses lose millions of shillings to BEC attacks each year. Finance teams are the primary target.

What to do:

- Enable multi-factor authentication (MFA) on all email accounts. This stops the majority of credential-based email takeovers
- Implement a verbal verification policy for any payment request received over email
- Configure email security policies to flag emails from outside your domain that claim to be from internal senders

3. Phishing & Credential Theft

Phishing emails trick employees into clicking malicious links or entering credentials on fake login pages. With KCB, Equity and M-Pesa branding widely trusted, attackers have effective local lures.

Modern phishing is highly targeted: attackers research your business on LinkedIn before crafting convincing impersonations of your bank, suppliers, or KPLC.

What to do:

- Train staff on phishing recognition: regular, simulated phishing tests are most effective
- Deploy email filtering with anti-phishing rules (Microsoft Defender, Google Workspace Advanced Protection)
- Use password managers and unique passwords for every service
- Enable MFA everywhere, especially on cloud services and banking platforms

4. Unsecured Cloud Storage

As businesses move to cloud storage (Google Drive, OneDrive, Dropbox), misconfigured access permissions are creating massive data exposure risks. A misconfigured S3 bucket or shared Google Drive folder can expose client contracts, employee records, and financial data to anyone on the internet.

What to do:

- Audit all cloud storage for public-facing access settings quarterly
- Enforce the principle of least privilege: staff should only access what they need for their role
- Enable data loss prevention (DLP) policies on cloud platforms
- Encrypt sensitive files before uploading to shared storage

5. Insider Threats & Poor Access Control

Not all threats are external. Disgruntled employees, contractors with excessive permissions, and accounts that aren't deprovisioned when staff leave are common attack vectors.

In Kenya's high staff-turnover environment (particularly in tech, banking and retail), this is a significant and underestimated risk.

What to do:

- Conduct quarterly access reviews: remove permissions for roles that have changed or left
- Implement a formal offboarding checklist that includes revoking all system access
- Log and monitor access to sensitive data, especially from privileged accounts
- Consider identity and access management (IAM) solutions for businesses with 20+ staff

The CloudSpinx Security Assessment

Most Nairobi SMEs we audit have never had an independent review of their security posture. Our cybersecurity assessment covers all five of the above threats, plus network security, data compliance, and employee security awareness, and we deliver a prioritized action plan within 7 days.

Book a free cybersecurity consultation →

Read next

All articles →

CYBERSECURITY 8 min

Where Your Servers Can Legally Live in East Africa

Data protection laws in Kenya, Tanzania, Uganda and Zambia decide...

CYBERSECURITY 13 min

Cybersecurity Threats Facing Kenyan Businesses

The 8 most common cyber attacks hitting Kenyan SMEs right now, with...

Amina Hassan 12 July 2026

Josphat Mutai 21 March 2026

IT STRATEGY 6 min

Choosing a Managed IT Provider in Kenya

Choosing a managed IT provider in Kenya without a ranked list: five thing...

CloudSpinx Team 6 September 2026