Last quarter we responded to 11 security incidents across Kenyan businesses. Nine of them could have been prevented with basic measures that cost less than KES 10,000/month. The other two were sophisticated attacks that required real expertise to contain - but even those started with someone clicking a link in an email.

CloudSpinx is a cybersecurity and managed IT provider based in Nairobi, Kenya. We run security audits and incident response for SMEs across East Africa. The patterns we see are consistent: Kenyan businesses are growing fast, adopting cloud tools, processing more digital payments, but security is always the last thing on the budget.

This post covers the 8 threats we see most often, with real examples from our work (anonymized), and practical defences you can implement this week.

The Threat Landscape for Kenyan Businesses in 2026

Before we get into specifics, here is the reality. Kenya's digital economy is booming. M-Pesa processes over KES 30 trillion annually. E-commerce is growing 25%+ year over year. eTIMS compliance pushed thousands of businesses online. But cybercrime is growing just as fast.

The Communications Authority of Kenya ↗ reported over 860 million cyber threat events detected in the 2024/2025 financial year. Most targeted small and medium businesses because they are the softest targets - valuable enough to steal from, not resourced enough to defend properly.

Here is what we are seeing in the field.

1. Business Email Compromise (the Biggest Threat)

This is not your typical spam. Business Email Compromise (BEC) is when an attacker gains access to a real business email account, or creates a convincing fake one, and uses it to redirect payments.

How it works in Kenya:

An attacker compromises the email of your supplier (or creates a lookalike domain like `supplier-ke.com` instead of `supplier.co.ke`). They send you an invoice that looks identical to the real thing, but with different bank account details. You pay. The money is gone.

Real incident we handled: A logistics company in Industrial Area received what appeared to be a routine invoice from their fuel supplier. The email came from the correct person's name, referenced the correct PO number, and the invoice format was identical. The only difference: the bank account was different. They paid KES 2.3 million to a fraudulent account. By the time they realized (three days later, when the real supplier asked about payment), the account had been emptied.

How to defend:

- Always verify bank account changes by phone. Call the supplier using a number you already have, not a number from the email.
- Enable DMARC, DKIM, and SPF ↗ on your email domain. This prevents attackers from spoofing your address.
- Use email filtering that flags external emails pretending to be internal senders.
- Train your finance team to pause before processing any payment where bank details have changed.

2. Ransomware Targeting Kenyan Servers

Ransomware encrypts all your files and demands payment (usually in cryptocurrency) to unlock them. It has hit Kenyan businesses hard in the past two years.

Why Kenyan SMEs are vulnerable: Many businesses run Windows servers with remote desktop (RDP) exposed to the internet. We have found RDP ports open on roughly 6 out of 10 Kenyan businesses we audit. That is an open door for ransomware gangs.

What it costs: The average ransom demand for Kenyan SMEs is USD 5,000 - 15,000 (KES 650,000 - 1.95 million). But the real cost is downtime. A business without backups can be offline for weeks. We have seen companies close permanently because they could not recover their data.

How to defend:

- Close RDP ports to the public internet. If you need remote access, use a VPN.

- Maintain offline backups. Cloud backups are good, but ransomware can encrypt those too if they are always connected. Keep one backup that is disconnected.
- Patch your servers. Most ransomware exploits known vulnerabilities that have patches available. If you are running Windows Server 2012 or 2016, you are at elevated risk.
- Deploy endpoint detection. CrowdStrike ↗ and SentinelOne ↗ are our recommendations for businesses that can afford them. For tighter budgets, Windows Defender for Business ↗ is surprisingly capable in 2026.

3. M-Pesa and Mobile Money Fraud

This is uniquely Kenyan. As businesses integrate M-Pesa into their payment flows, new attack surfaces open up.

Common patterns we see:

- **SIM swap attacks:** An attacker convinces Safaricom to transfer your phone number to their SIM. They then access your M-Pesa business account and drain it.
- **Fake payment confirmations:** Customers show you a forged M-Pesa confirmation SMS. The money never actually moved.
- **API key theft:** If you use the Daraja API ↗ for M-Pesa integration, stolen API credentials let attackers initiate transactions from your business account.

How to defend:

- Register for Safaricom's SIM swap notification service. You get an SMS when anyone attempts a SIM swap on your number.
- Never trust screenshot confirmations. Always verify payments through your M-Pesa business portal or Daraja API callbacks.
- Store Daraja API keys in environment variables or a secrets manager, never in code or configuration files that developers can see.
- Use M-Pesa's IP whitelisting to restrict API access to your servers only.

4. Phishing Attacks Targeting Staff

Classic phishing remains the number one entry point for most attacks. In Kenya, we see phishing emails that impersonate KRA, Safaricom, banks, and Google.

The most effective phishing emails we have seen in Kenya:

- "Your KRA PIN is about to expire. Click here to renew." (KRA does not send renewal emails with login links.)
- "Safaricom Fibre: your bill is overdue. Update payment method." (Links to a fake Safaricom portal that steals credentials.)
- "Shared document: Q3 Financial Report.xlsx" from what appears to be a colleague's Google account.

A 2026 twist: Attackers are now using AI to write phishing emails in perfect Swahili and Sheng, targeting businesses that would previously have been filtered by poor English.

How to defend:

- Run phishing simulations. Send your own fake phishing emails to staff and track who clicks. The first round is always shocking - expect 30-40% click rates. After 3 months of training, it drops to under 5%.
- Enable 2FA on every account. Google Workspace, Microsoft 365, banking portals, social media. All of them.
- Use a password manager (Bitwarden ↗ is free and excellent) so staff do not reuse passwords across services.

5. Insider Threats and Departing Employees

Not every threat comes from outside. Departing employees who still have access to company systems are a real risk.

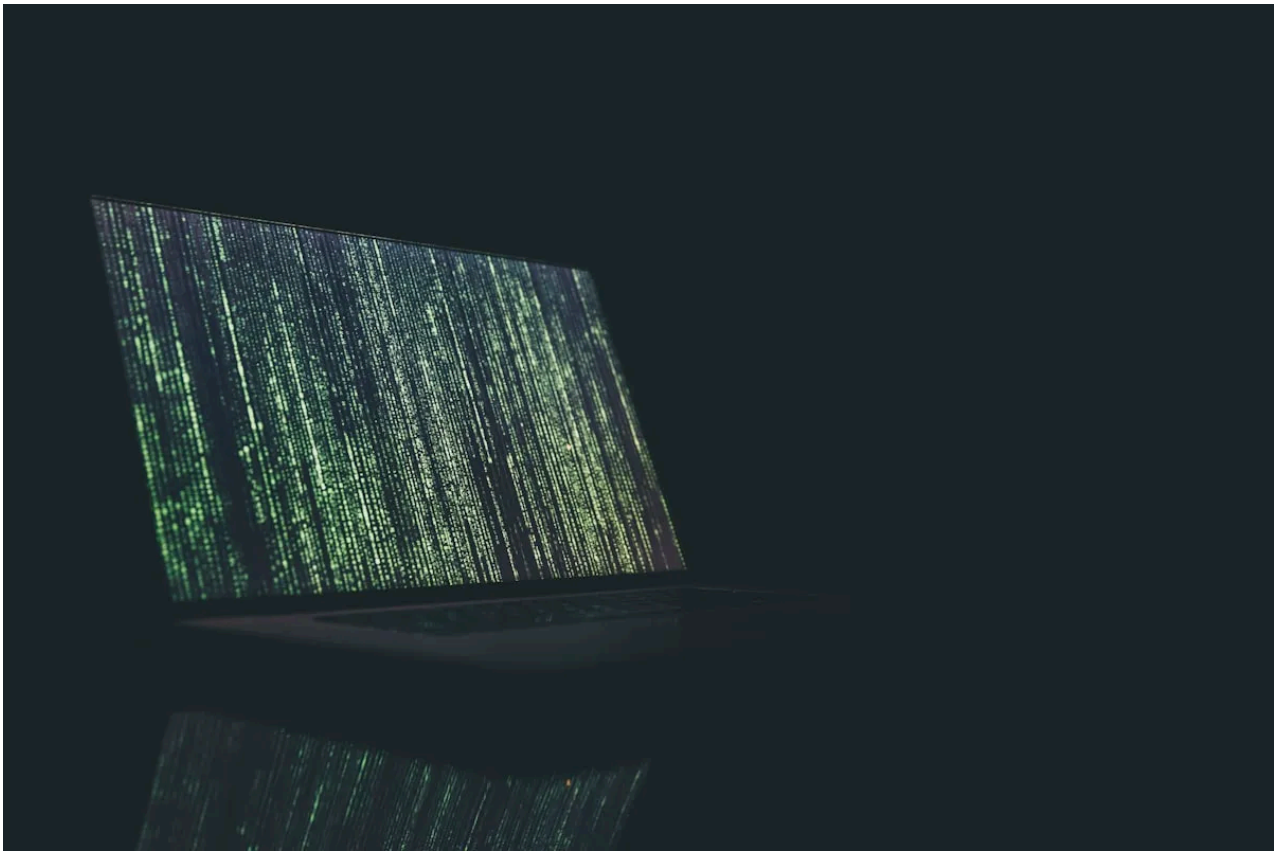
What we see: A staff member resigns or is fired. Nobody disables their Google Workspace account, their access to the accounting system, or their VPN credentials. Weeks later, data is accessed, deleted, or copied.

Real incident: A sales manager at a Nairobi distribution company was fired. His Google account stayed active for 47 days. During that time, he downloaded the

entire customer database (3,400 contacts with purchase history) and took it to a competitor.

How to defend:

- Create an offboarding checklist: disable accounts within 1 hour of termination, revoke VPN access, change shared passwords, recover company devices.
- Use Google Workspace's admin tools ↗ to remotely wipe company data from personal devices.
- Restrict who can export customer databases and financial records. Not every employee needs download access.



6. Unsecured Wi-Fi and Office Networks

We audit office networks across Nairobi and the findings are predictable. Default router passwords, guest Wi-Fi on the same network as business systems, no network segmentation.

Why this matters: If an attacker gets on your Wi-Fi (which is easy if the password is "companyname2024"), they are inside your network. From there, they can

access shared drives, intercept traffic, and move to servers.

How to defend:

- Change default router and access point passwords. Use WPA3 if your hardware supports it.
- Create separate VLANs for guest Wi-Fi, staff devices, and servers. Guest traffic should never touch your business network.
- Disable WPS (Wi-Fi Protected Setup) on all access points - it is trivially hackable.
- Our network and connectivity services include full network segmentation and firewall configuration.

7. Unpatched Software and End-of-Life Systems

We still find Windows 7, Windows Server 2012, and CentOS 7 running in Kenyan production environments. All three are end-of-life, meaning they receive zero security updates. Every known vulnerability is permanently exploitable.

The most dangerous unpatched systems we find:

- Microsoft Exchange Server 2016 without the latest cumulative updates
- WordPress sites running plugins that have not been updated in 2+ years
- PHP 7.x on web servers (end-of-life since November 2023)
- Ubuntu 18.04 LTS (end-of-life since May 2023)

How to defend:

- Inventory every piece of software in your business. If it is end-of-life, make a plan to replace it.
- Enable automatic updates where possible.
- For servers, schedule a monthly maintenance window for patching. Our Linux infrastructure and Windows Server teams handle this as part of managed services.

8. Cloud Misconfiguration

As Kenyan businesses move to the cloud, a new category of risk emerges: misconfigured cloud services.

What we find:

- S3 buckets (AWS file storage) left publicly accessible with customer data inside
- Google Workspace sharing settings that allow anyone with a link to access company documents
- Database servers (PostgreSQL, MySQL) exposed to the internet with default ports and weak passwords
- No encryption on data at rest or in transit

Real incident: A Kenyan e-commerce company stored customer payment records in an AWS S3 bucket that was publicly accessible. It was indexed by automated scanners within hours. Customer names, phone numbers, and partial M-Pesa details were exposed. The company only discovered it when a security researcher reached out.

How to defend:

- Run a cloud security audit before going live. We do this as part of every cloud infrastructure deployment.
- Enable AWS GuardDuty, Azure Security Center, or Google Security Command Center to automatically detect misconfigurations.
- Never use default database ports (5432 for PostgreSQL, 3306 for MySQL) on internet-facing servers.
- Encrypt everything. At rest (AES-256) and in transit (TLS 1.2+).

What a Basic Security Setup Costs for a Kenyan SME

You do not need a SOC (Security Operations Center) or a full-time security team. Here is what actually protects a small business:

DEFENCE	MONTHLY COST (KES)	WHAT IT COVERS
Google Workspace / M365 with 2FA	850 - 1,700/user	Email security, access control
Password manager (Bitwarden)	Free - 500/user	Credential management
Endpoint protection (Defender for Business)	400 - 800/user	Malware, ransomware detection
Email filtering (built into Workspace/M365)	Included	Phishing, spam blocking
Automated cloud backups	1,500 - 5,000	Data recovery
Quarterly phishing simulation	5,000 - 15,000	Staff awareness
Annual security audit	8,000 - 25,000/month amortized	Vulnerability assessment
Total for 10-person company	**KES 20,000 - 50,000/month**	

Compare that to the cost of a single ransomware incident (KES 650,000+) or a BEC payment fraud (millions). Security is the cheapest insurance you can buy.

The 15-Minute Security Checklist

If you do nothing else after reading this, do these 7 things. They will eliminate 80% of your risk.

1. **Enable 2FA on all email accounts.** Google Workspace and Microsoft 365 both support it. Takes 10 minutes per user.
2. **Check if RDP is exposed.** Ask your IT person: "Is Remote Desktop accessible from the internet?" If yes, close it immediately and set up a VPN.
3. **Verify your backup actually works.** Do not just check that the backup job ran. Actually restore a file from the backup. If you cannot, you do not have a backup.
4. **Update your operating systems.** If anything is running Windows 7, Windows Server 2012, or Ubuntu 18.04, it needs to be replaced.
5. **Change default router passwords.** Including the Wi-Fi password if it is still the ISP default.
6. **Create an offboarding process.** When someone leaves, disable their accounts the same day.
7. **Talk to your team about phishing.** A 15-minute conversation about what phishing looks like is better than nothing.

Frequently Asked Questions

What are the biggest cybersecurity threats for Kenyan businesses in 2026? Business email compromise (BEC), ransomware, M-Pesa fraud, phishing attacks, and insider threats are the top five. BEC is the most financially damaging, with Kenyan businesses losing millions in KES to fraudulent invoice payments. Ransomware is the most operationally devastating, capable of shutting down a business for weeks.

How much does cybersecurity cost for a small business in Kenya? A basic security setup for a 10-person Kenyan SME costs KES 20,000 - 50,000/month. This covers email security with 2FA, endpoint protection, automated backups, and quarterly phishing simulations. CloudSpinx offers cybersecurity packages starting from KES 25,000/month for small businesses.

How do I protect my business from phishing in Kenya? Enable two-factor authentication on all accounts, run quarterly phishing simulations to train staff, use a password manager like Bitwarden, and configure DMARC/DKIM/SPF on your email domain. Most phishing attacks succeed because staff are not trained to recognize them, not because the technology failed.

Is M-Pesa safe for business transactions? M-Pesa itself is secure, but the integration points create risk. Protect your Daraja API keys, use IP whitelisting, register for SIM swap notifications, and never accept screenshot payment confirmations. Always verify transactions through your M-Pesa business portal.

Do I need a cybersecurity team for my small business? No. Most Kenyan SMEs with under 50 employees do not need a dedicated security person. A managed IT provider like CloudSpinx handles security monitoring, patching, and incident response as part of managed services. This is cheaper and more effective than a single in-house hire who cannot cover 24/7.

What should I do if my business is hacked? Disconnect affected systems from the network immediately. Do not pay ransoms. Contact your managed IT provider or a security incident response team. Preserve evidence (do not wipe systems). Notify affected customers if personal data was compromised. Kenya's Data Protection Act ↗ requires breach notification.

Getting Started

Cybersecurity does not have to be complicated or expensive. Start with the 15-minute checklist above. If you want a professional assessment, we offer a free security audit that covers your email configuration, network exposure, backup status, and the most critical vulnerabilities.

Book a free security audit or reach out on WhatsApp at +254 713 403 044. We will tell you exactly where your risks are and what to fix first. See our full cybersecurity services for details on ongoing protection.

Read next

All articles →

CYBERSECURITY 6 min

The 5 Biggest Cyber Threats Facing Nairobi SMEs Right Now

Ransomware, phishing and credential theft are rising sharply in Kenya. Here...

Amina Hassan 15 March 2026

EMAIL 9 min

Why Your Business Email Still Runs on Free Gmail (and Why That Is Costing You)

Most Kenyan SMEs send invoices and tender responses from personal Gmai...

Amina Hassan 23 March 2026

DEVOPS 11 min

Your Developers Are Deploying Code Over SSH: A CI/CD Wake-Up Call for Kenyan Tech Companies

Most Kenyan dev teams still deploy by SSHing into production. We break do...

Josphat Mutai 23 March 2026