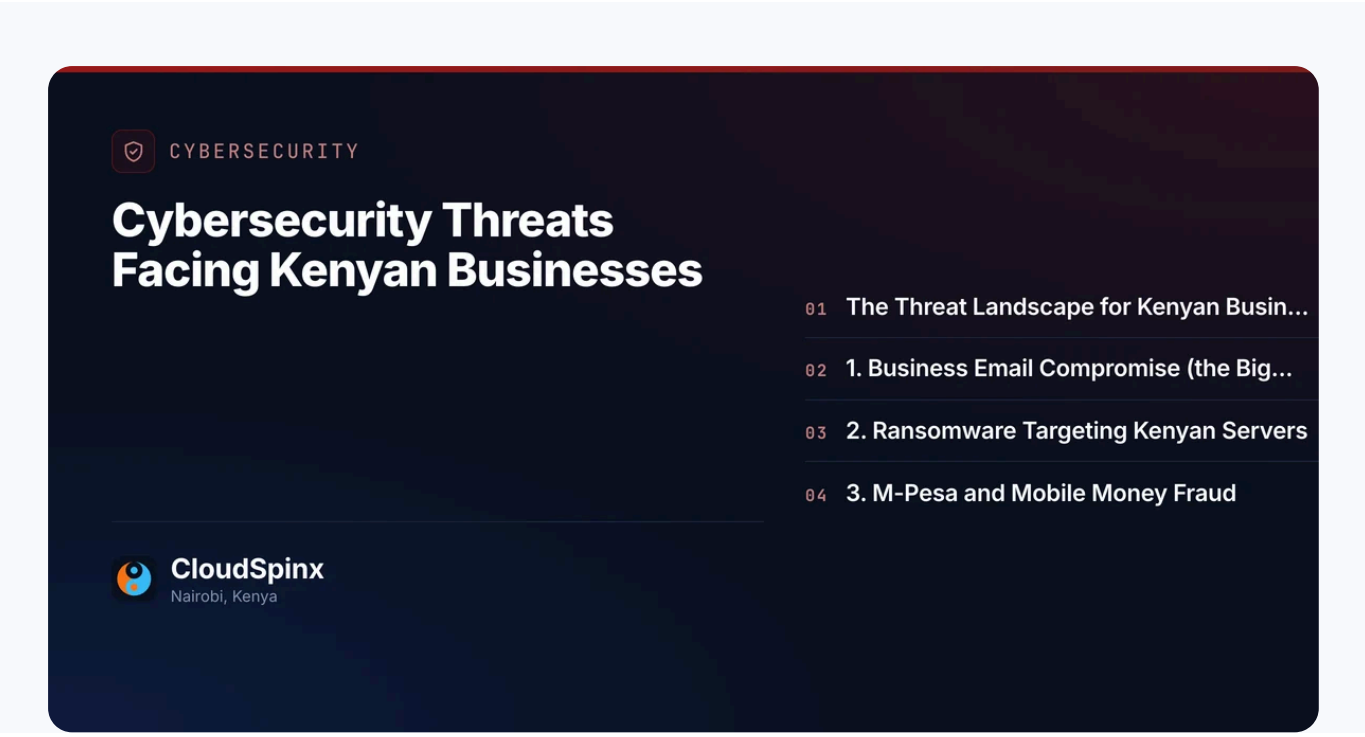

CloudSpinx Kenya cloudspinx.co.ke

Most attacks that hurt Kenyan businesses are not clever. A supplier invoice with one changed field. A Remote Desktop port open to the whole internet. A sales manager whose email still works three weeks after he left. The expensive incidents usually start with somebody clicking a link.

The eight threats below are the ones we plan defenses around first when CloudSpinx runs security audits and incident response for organizations in Kenya and across East Africa.

The Threat Landscape for Kenyan Businesses

M-Pesa processed KES 41.68 trillion in Safaricom's 2026 financial year, about 2.4 times Kenya's GDP by Safaricom's own annual report ↗. eTIMS moved tax invoicing online. Money that moves through phones, APIs and email is money an attacker can redirect without ever touching your premises.

The Communications Authority of Kenya ↗'s National KE-CIRT/CC detected about 8.6 billion cyber threat events across the 2024/25 financial year (July 2024 to June

2025), summed from its quarterly reports ↗. The CA does not break that down by business size. Our read: small and medium businesses are the softest targets, valuable enough to steal from and rarely resourced to defend.

1. Business Email Compromise

Business Email Compromise (BEC) is an attacker using a real business mailbox, or a convincing fake one, to redirect a payment. Nothing about it looks like spam.

The usual route: your supplier's email is compromised, or someone registers a lookalike such as `supplier-ke.com` for `supplier.co.ke`. You receive the invoice you pay every month. Correct sender name, correct PO number, the usual layout and amount. One field has changed, and it is the bank account. The fraud surfaces when the real supplier chases payment, and by then the receiving account is empty.

The defense is a process before it is a product. Any change of bank details gets confirmed by phone, on a number you already hold, never one from the email. Finance staff are told, in writing, that pausing a payment for that call is never the wrong decision. Then the technical half: publish SPF, DKIM and DMARC ↗ for your own domain so nobody can send as you, and turn on the external-sender warning in Google Workspace or Microsoft 365 so a message from outside that claims to be internal is flagged.

2. Ransomware Targeting Kenyan Servers

Ransomware encrypts your files and demands payment, usually in cryptocurrency, to unlock them. The ransom is rarely the real cost. Downtime is, and a business with no clean backup can be offline until it rebuilds from scratch.

Two doors deserve closing first: Remote Desktop exposed to the internet on a Windows server, and known vulnerabilities on systems nobody has patched. Close RDP to the public internet and put remote access behind a VPN. Keep one backup copy that ransomware cannot reach: offline, or in a separate account with credentials the production servers never hold, because a backup share that is always mounted gets encrypted with everything else. Patch on a schedule, and

treat anything still on Windows Server 2012 as an emergency, since it is past end of support.

For endpoint detection, CrowdStrike and SentinelOne are what we recommend when the budget allows. For a smaller team, Microsoft Defender for Business does real detection and response for up to 300 users, and it is already included in Microsoft 365 Business Premium, which a lot of offices pay for without switching it on.

3. M-Pesa and Mobile Money Fraud

This one is ours. As businesses wire M-Pesa into their payment flows, three attacks follow.

A SIM swap moves your number to the attacker's SIM, and with it the one-time codes that guard your business accounts. A forged confirmation SMS or screenshot convinces a cashier that money arrived when it never did. And stolen Daraja API credentials let someone transact against your business shortcode.

Treat a phone that suddenly loses network as an incident, and call Safaricom from another line before you do anything else. Never release goods on a screenshot or an SMS: confirm the payment in the M-Pesa business portal or from your own Daraja callback. Keep the Daraja consumer key and secret in a secrets manager or environment variables, out of the code repository and out of any config file a developer can read. And do not trust a callback on sight; query the transaction status before you fulfill an order.

4. Phishing Attacks Targeting Staff

Phishing needs no vulnerability at all, only a person. The lures that work in Kenya borrow a brand people already trust:

- "Your KRA PIN is about to expire. Click here to renew." KRA PINs do not expire, and KRA does not send login links.
- "Your fibre bill is overdue. Update your payment method." The link goes to a fake provider portal that collects card details or credentials.

- "Shared document: Q3 Financial Report.xlsx" from what looks like a colleague's Google account.

Language is no longer a filter either. Generative tools write clean Swahili as easily as English, so a badly worded email is no longer the giveaway staff were taught to look for.

Run phishing simulations, so the first click happens on a test rather than a real attack, and repeat them until the click rate stops embarrassing anyone. Turn on two-factor authentication on every account that offers it, email first. Give staff a password manager such as Bitwarden ↗ so one breached password does not open five services.

5. Insider Threats and Departing Employees

Not every threat comes from outside. The common case is mundane: someone leaves, and nobody disables their Google Workspace account, their accounting login or their VPN profile. Weeks later the customer list is in a competitor's CRM.

Disable accounts the same hour a person leaves, then revoke VPN access, rotate any shared passwords and recover company devices. Google Workspace's admin console ↗ can wipe company data from a personal phone. And restrict who can export the customer database and the financial records at all. Most staff never need a download button.

If personal data does leave, the clock starts. Section 43 of Kenya's Data Protection Act ↗ requires the data controller to notify the Data Commissioner within seventy-two hours of becoming aware of a breach that carries a real risk of harm, and to tell the affected people in writing.

6. Unsecured Wi-Fi and Office Networks

Default router passwords, guest Wi-Fi on the same network as the accounts PC, no segmentation. If the Wi-Fi password is the company name and a year, anyone in the car park is inside your network, with a path to the shared drives and the servers.

Change every default password on routers and access points, and use WPA3 where the hardware supports it. Put guests, staff devices and servers on separate VLANs so guest traffic never touches the business network. Disable WPS on every access point; its PIN can be brute-forced. Our network and connectivity services do the segmentation and firewall work end to end.

7. Unpatched Software and End-of-Life Systems

Windows 7, Windows Server 2012 and CentOS 7 still turn up in Kenyan production environments. An end-of-life system gets no security updates, so every vulnerability found after its last patch stays open for good. The ones that matter most right now:

- Exchange Server 2016 and 2019, both out of support ↗ since October 14, 2025
- PHP 7.4, end of life ↗ since November 28, 2022, still running under a lot of WordPress sites with plugins nobody has updated
- Ubuntu 18.04, whose standard security maintenance ended in May 2023 ↗
- CentOS 7, end of life since June 30, 2024

Inventory what you run, put an end date next to each item, and plan the replacements before the dates pass rather than after. Turn on automatic updates where they are safe. For servers, a monthly patch window beats patching whenever someone remembers; our Linux infrastructure and Windows Server services run that window for you.

8. Cloud Misconfiguration

Moving to the cloud swaps one set of risks for another. The usual mistakes: a storage bucket left public with customer files in it, Google Workspace sharing set to "anyone with the link", and a PostgreSQL or MySQL server reachable from the internet with a weak password. Automated scanners find exposures like these quickly, and the owner usually hears about it from a stranger.

A database should not be reachable from the internet at all; moving it off the default port is not a control. Keep it on a private network and let the application reach it there. Encrypt data at rest and in transit. Then switch on the provider's own posture

checks (AWS Security Hub, Microsoft Defender for Cloud, Google Security Command Center), which flag public buckets and open ports as they appear. We run a security review before go-live on every cloud infrastructure deployment.

What a Basic Security Stack Is Made Of

You do not need a security operations center or a full-time security hire. Most of a small business's protection is licensing it already pays for, switched on properly, plus a few habits.

DEFENSE	WHERE IT COMES FROM	HOW IT IS PRICED
Two-factor authentication and email filtering	Google Workspace or Microsoft 365, built in	Inside the per-user subscription you already pay
Endpoint detection and response	Microsoft Defender for Business, included in Microsoft 365 Business Premium or sold standalone	Per user
Password manager	Bitwarden business plans, or similar	Per user, billed annually
One backup copy ransomware cannot reach	A separate storage account or offline media	By capacity
Phishing simulation and a yearly audit	A security provider	Quoted per engagement

What it costs your business depends on headcount and what you already license, so we quote it from your environment rather than a rate card.

The 15-Minute Security Checklist

If you do nothing else after reading this, do these seven things this week.

1. **Turn on two-factor authentication for every email account.** Google Workspace and Microsoft 365 both support it.
2. **Find out whether Remote Desktop is open to the internet.** Ask whoever runs your IT. If it is, close it and set up a VPN.
3. **Restore one file from your backup.** Do not just check that the job ran. If you cannot restore, you do not have a backup.
4. **List anything running an end-of-life system** (Windows 7, Windows Server 2012, Ubuntu 18.04, CentOS 7) and put a replacement date next to it.
5. **Change default router and Wi-Fi passwords**, including the Wi-Fi password your ISP set at installation.
6. **Write a one-page offboarding process.** When someone leaves, their accounts close the same day.
7. **Spend fifteen minutes with your team on what phishing looks like.** Show them the KRA lure above.

When that is done, a proper review covers your email configuration, network exposure, backup status and the vulnerabilities that matter most. Book a free consultation or message us on WhatsApp at +254 713 403 044, and we will tell you where your risks are and what to fix first. Ongoing protection is on the cybersecurity services page.

Read next

All articles →

CYBERSECURITY 7 min

MongoDB Backup Encryption: Dumps and Logs Stay Readable

MongoDB backup encryption, tested: under LUKS and under Percona's...

CloudSpinx Engineering 26 October 2026

CYBERSECURITY 8 min

Where Your Servers Can Legally Live in East Africa

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

Amina Hassan 12 July 2026

CYBERSECURITY 4 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