FOXTROT SHIELD
ANTICIPATE. PROTECT. PREVAIL.

RISK ADVISORY

FOXTROT SHIELD INSIGHTS

Five Security Risks Nigerian Businesses Should Plan for in 2026

A practical guide for leaders, HR teams and operations managers preparing for insider threat, executive safety, cyber-enabled fraud, vendor risk and crisis disruption.

Foxtrot Shield Intelligence Team 2026 Risk Advisory

The Nigerian operating environment rewards preparation. For business leaders, HR teams and operations managers, the question is not whether risk will appear. It is whether the organisation is ready to absorb it without losing control.

01 Insider threat and employee fraud

As hiring grows, so does exposure to fraud, data misuse and deliberate disruption from within an organisation. Informal reference checks are rarely enough, especially for roles with access to money, systems, client data or sensitive operations.

WHAT TO DO

Make structured screening part of the hiring process. Employment verification, education checks and professional reference validation should be standard, with equivalent due diligence for contractors and vendors.

02 Kidnap for ransom and executive safety

Kidnap-for-ransom remains a serious concern in parts of Nigeria. Executives and high-profile staff can be exposed through travel routines, public visibility and movement through higher-risk corridors.

WHAT TO DO

Assess travel risk for senior staff, establish journey management protocols, vary predictable routines and give leadership teams practical personal security awareness training.

03 Cyber-enabled fraud and social engineering

Business email compromise, phishing and social engineering continue to be common routes into financial fraud. Many attacks do not rely on advanced technical skill; they rely on urgency, trust and distraction.

WHAT TO DO

Treat security awareness as an organisational issue, not only an IT issue. Train staff regularly, strengthen payment verification rules and make suspicious activity easy to report.

04 Vendor and third-party risk

A company can be exposed by the weakest party in its supply chain. Contractors, service providers and commercial partners can create financial, reputational and operational risk when they are not properly vetted.

> **WHAT TO DO**
>
> Create a vendor due diligence process covering background checks, financial health, ownership, references and periodic review, especially where regulated work or donor funding is involved.

05 Crisis unpreparedness

Many organisations still operate without a tested continuity plan, crisis communication protocol or incident response playbook. When disruption happens, the absence of a plan can become the largest risk of all.

> **WHAT TO DO**
>
> Review critical functions, map dependencies and rehearse response roles. A tabletop exercise is a practical way to reveal gaps before a real incident does.

Preparedness is a management discipline.

Organisations that navigate 2026 well will not simply be the largest or best resourced. They will be the ones that understand their exposure, assign responsibility and practise their response before a disruption tests them.