GRCPRENEUR EVIDENCE REPORT

2026 cyber threat reports: decisions for a small business

Prepared for GRCPreneur by Hassan Sharif | Source review: 19 November 2026

Purpose, evidence and limits

This GRCPreneur evidence brief brings selected 2026 publications into a small-business decision discussion. It is desk-based commentary, not a survey of Kenyan businesses, a prediction of an individual firm's losses or a report of client work. Sources were checked on 19 November 2026.

Kenya's Communications Authority reports 2,696,335,021 detected cyber threat events for July-September 2026, up 14.45% on the preceding quarter. These are reported threat events, not a count of successfully breached businesses or unique victims. [1]

ENISA's September 2026 publication examines incidents observed during January-December 2025 and highlights digital dependencies. [2] The UK NCSC's November 2026 review discusses familiar weaknesses and the importance of preparation. [3] NIST's November 2026 guide addresses firms with no employees other than the owner. [4]

These publications have different populations, periods and purposes. Their figures should not be added together or converted into a probability for a Kenyan SME. The useful common question is which business dependency deserves a clearer owner, safeguard or recovery arrangement.

The recommendations that follow are GRCPreneur's interpretation. They organise a management conversation; they do not prescribe a universal sequence, spending level or completion deadline.

2026 cyber threat reports: decisions for a small business

Four decisions to take from the evidence

Identify an activity whose interruption matters

Choose a real activity such as receiving orders, arranging appointments or completing client work. Name the information, accounts and suppliers it needs. Explain the first material consequence of losing access. This establishes a useful boundary for reviewing a national or international threat theme.

Give maintenance and access an accountable owner

Ask who receives supplier notifications, who decides whether a change is urgent, who performs the authorised work and how completion is checked. Keep a proposed improvement separate from one implemented and verified. A small firm can start with one essential service rather than an unmanageable inventory of every possible weakness.

Examine a dependency beyond the main supplier

An email account may control recovery for the booking service; an outside developer may administer the domain. Draw the practical connection. Ask what happens if that account, person or provider is unavailable. Treat a previously unnoticed dependency as a question to resolve, rather than assuming a second supplier automatically provides independence.

Make the next decision visible

Record the concern, evidence available, material uncertainty, options, decision owner and next review point. The result might be an agreed access-recovery check, a supplier clarification or a policy change. A report has helped only when the business can explain what it will do with the information.

Choose actions according to the business consequence, feasibility and unresolved exposure. Avoid treating the largest number in a threat report as the automatic highest priority for every firm.

2026 cyber threat reports: decisions for a small business

Fictional example: a booking service and its recovery route

A small consultancy depends on a hosted appointment service. Its owner has read about growing cyber threats and is considering another security subscription. Before choosing a product, the owner describes the work that would stop if appointments became unavailable.

The discussion identifies three dependencies: the booking provider, a business email account and a recovery phone held by an occasional contractor. Backups may exist, but the owner has not confirmed how access would be recovered if the contractor could not be reached.

The immediate decision is to clarify ownership and authorised recovery options with the provider. The technical owner will plan any change, preserve a working route and document an appropriate check. A separate discussion will address restoring appointment records and temporary customer communication.

This fictional example does not claim that a breach happened, that a product is unnecessary or that a recovery test succeeded. It illustrates how a broad threat theme can produce a specific management question.

The proposed completion record names what was checked, the supporting evidence reference and what remains unresolved. The owner can then reconsider the original spending proposal with a clearer understanding of the dependency.

2026 cyber threat reports: decisions for a small business

A practical starting record

For one essential activity, write down:

- The service, information and dependencies needed to keep working.

- The concern the report prompted you to examine.

- What is known, what is assumed and what needs confirmation.

- The available response options and who can approve them.

- The next action, responsible person and completion evidence.

- The date or change that will trigger another review.

Use the Cybersecurity Risk Register Worksheet for the business exposure and the Critical Account Recovery Planning Worksheet for access dependencies. Keep passwords, recovery codes and sensitive system details in protected storage, outside these discussion records.

Review the original sources before relying on a statistic. A national detection total is context; your own service, evidence and responsibilities determine the decision you need to make.

Sources reviewed

[1] Communications Authority of Kenya: Cyber Security Report Q1 FY 2026-2027 (July-September 2026)

[2] ENISA Threat Landscape 2026

[3] NCSC Annual Review 2026: 7 things we learned

[4] NIST CSWP 50: Small Business Cybersecurity: Non-Employer Firms

Your next decision

Business question	
Decision owner	
Evidence still needed	
Next action / review	