



WHITEPAPER

Ransomware Readiness: A Field Playbook for East African Enterprises

The decisions that determine whether a ransomware event is a bad week or an existential one — and which of them have to be made before the encryption starts.

PUBLISHED

February 11, 2026

READING TIME

14 minutes

AUTHOR

SCIAT AFRICA Research

ABSTRACT

Ransomware rarely fails because of the malware. It succeeds because of backup architecture that was never restore-tested, flat internal networks, administrative accounts shared between IT and OT, and an incident plan that lives in a document nobody has opened. This playbook sets out the controls and rehearsals that change the outcome, written for organisations operating in Kenya and the wider East African region.

Topics: Ransomware · Incident Response · Business Continuity

WHAT TO TAKE AWAY

- An immutable or offline backup copy is the single control most strongly correlated with recovery without payment.
- Restore time, not backup time, is the number that matters — and it is only knowable by rehearsing a restore.
- Flat networks convert a single compromised endpoint into a whole-estate event; segmentation buys containment time.
- Kenya's Data Protection Act obliges notification to the Data Commissioner within 72 hours of becoming aware of a qualifying breach, which means legal review belongs in the first day, not the second week.
- The decision on whether to pay should be a pre-agreed board position, taken calmly, not an operational judgement taken at 3am.

CONTENTS

- 01** Why the malware is the least interesting part
- 02** Backups: the only control that reliably changes the ending
- 03** Segmentation buys the time everything else needs
- 04** The first twenty-four hours
- 05** Deciding about payment before you have to
- 06** A readiness checklist

01 Why the malware is the least interesting part

By the time a ransom note appears, the attacker has usually been inside the environment for days or weeks. The encryption is the closing act of an intrusion that began with a stolen credential, an exposed remote-access service, or a phishing email that was clicked and never reported. Investigating the encryptor tells you which affiliate programme you are dealing with. Investigating the access path tells you how to stop it happening again.

That distinction shapes everything about preparation. Controls aimed at the encryption event – antivirus signatures, file-extension blocklists – operate at the point of least leverage. Controls aimed at the access path and at lateral movement operate where the attacker is still constrained, still noisy, and still reversible.

02 Backups: the only control that reliably changes the ending

The conventional 3-2-1 rule – three copies, on two media types, with one off-site – predates ransomware, and modern operators have adapted to it. They look for the backup server, they look for the credentials that reach it, and where they find network-reachable backups under the same directory domain as production, they destroy them first. A backup that an administrator account can delete is a backup an attacker can delete.

What survives is a copy the production environment cannot reach or alter: offline media, or object storage with an enforced immutability window that even the account owner cannot shorten. The retention window needs to exceed your realistic detection time, because a backup taken after the intrusion began may already contain the attacker's persistence.

And a backup is a hypothesis until it is restored. Restore rehearsal surfaces the problems that only appear under load – undocumented application dependencies, licence keys held by one person, database consistency requirements, bandwidth limits that turn a four-hour estimate into a four-day reality.

- Hold at least one copy that production credentials cannot modify or delete.
- Set the immutability window longer than your worst-case detection time.
- Rehearse a full restore of a tier-one system at least twice a year, and time it.
- Keep the restore runbook outside the systems it restores.

03 Segmentation buys the time everything else needs

Most enterprise networks in the region remain substantially flat behind the perimeter: a workstation that can reach a domain controller can also reach the finance file share, the virtualisation console

and the backup appliance. Under those conditions one compromised laptop is an estate-wide event, and the defender has no interval in which to act.

Segmentation does not have to mean a zero-trust rebuild. The high-value first pass is to isolate the four asset classes that convert a local compromise into a total one: identity infrastructure, virtualisation and hypervisor management, backup infrastructure, and any operational-technology network. Administrative access to each should require a separate credential and a separate path.

04 The first twenty-four hours

NIST SP 800-61 structures incident handling as preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. The failure mode we see most often is a jump straight from detection to eradication – machines reimaged before anyone has established the access path, destroying the evidence needed to know whether the attacker still holds a way back in.

Containment and evidence preservation are not in tension if the sequence is planned. Isolate at the network layer rather than powering down, so volatile memory survives. Capture disk and memory images of the first-identified hosts before remediation touches them. Preserve authentication and remote-access logs immediately, since those are usually the first to roll over.

Legal and regulatory review starts on day one, not after recovery. Under section 43 of Kenya's Data Protection Act, 2019, a data controller must notify the Data Commissioner without delay and within seventy-two hours of becoming aware of a breach where there is a real risk of harm to a data subject, and communicate with affected data subjects in writing. Sector regulators add their own expectations – the Central Bank of Kenya's Guidance Note on Cybersecurity for the Banking Sector sets reporting obligations for supervised institutions, and licensees under the Communications Authority coordinate with the National KE-CIRT/CC.

05 Deciding about payment before you have to

Payment is a business decision with legal, ethical and practical dimensions, and it is a poor one to make under duress at three in the morning. Boards that have taken a documented position in advance – including the circumstances in which they would reconsider, who is authorised to decide, and what sanctions screening is required first – act faster and more coherently than boards that have not.

The practical argument against payment has strengthened as double-extortion has become standard: paying may buy a decryption key, but it does not reliably buy deletion of exfiltrated data, and it does not remove the attacker's access. The organisations we have seen recover best are those that could restore, and therefore negotiated from a position where payment was genuinely optional.

06 A readiness checklist

None of the following requires a new platform purchase. All of it requires someone to own it and a date by which it is done.

- Multi-factor authentication on every remote-access path and every administrative account, with no exception list.
- An inventory of internet-exposed services, reviewed monthly against what is intended to be exposed.
- One backup copy that production cannot alter, with a tested restore and a recorded restore time.
- Administrative tiering that separates identity, hypervisor, backup and OT access.
- Centralised logging with a retention period longer than your detection time, held somewhere the attacker cannot reach.
- A named incident lead, a named legal contact, a named communications owner, and a contact route for each that works when corporate email does not.
- An annual tabletop exercise that includes the board, not only the technical team.

About this publication

This document is published by SCIAT AFRICA, a cybersecurity and digital forensics agency based in Nairobi, Kenya. It is free to read, print and circulate inside your organisation. The web edition, which carries the same content, is at <https://sciatafrica.com/research/ransomware-readiness-playbook>.

It is general guidance, not legal advice and not a substitute for an assessment of your own environment. Where it refers to a law, regulation or standard, read the instrument itself before relying on it – and talk to us if you want help applying it to your estate.

SCIAT AFRICA

info@sciatafrica.com · +254 794 946633 · <https://sciatafrica.com>