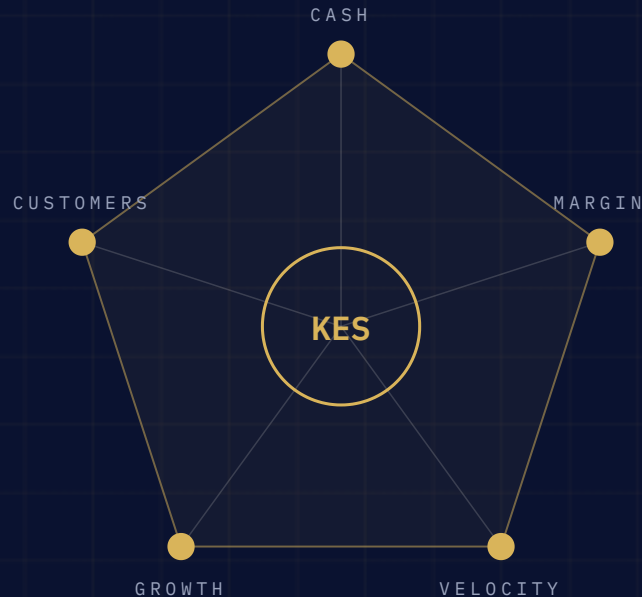




KNOW THE BUSINESS

You Cannot Defend What You Cannot Price

The most respected security frameworks start with the business. Most security training starts with the tools.

A finding with a severity score asks for attention. A finding with a shilling figure asks for a decision.

KEY FINDINGS

- Leading frameworks, NIST CSF 2.0 and PASTA among them, start with the business, not the technology.
- A severity score asks for attention; frequency times cost, in shillings, asks for a decision.
- Kenya's DPA requires breach notification within 72 hours and caps fines at KES 5m or 1% of turnover, whichever is lower.

Ask a newly trained analyst what a savings co-operative must protect, and the answer usually lists systems: the core banking server, the network, the email. Ask the co-operative's manager the same question and the answer is money, members and the month-end. This essay argues that a defender who cannot describe how a business makes money, and what an hour of failure costs it, is doing IT rather than security, and that the leading frameworks have been saying so for years.

01 Where the frameworks begin

The NIST Cybersecurity Framework 2.0 opens its Govern function with organisational context: the organisation's mission, its stakeholders and their expectations, its legal and contractual obligations, and the objectives, capabilities and dependencies that the mission relies on [1]. The PASTA threat-modelling method makes the same move at its first stage, which is to define business objectives before any technical scope is drawn [2]. Neither framework treats the business as background. Both treat it as the first input.

The reason is practical. Without a model of what the business values, every finding looks equally urgent, and a security team ends up defending infrastructure rather than outcomes.

02 The owner's language

Ram Charan observed that every business, from a street vendor to a multinational, runs on the same few things: cash, margin, velocity, growth and customers [3]. A vegetable seller in a Nairobi market manages all five in her head every day. She knows what she paid, what she can charge, how fast stock must move before it spoils, and which customers come back. A defender who understands a business at that level can explain a risk in terms its owner already uses.

Jack Freund and Jack Jones gave that explanation a method. Factor Analysis of Information Risk expresses risk as how often a loss is likely to happen multiplied by how large it would be, in money [4]. A vulnerability score tells a manager that something is severe. A frequency and a magnitude tell them what it is worth spending to prevent.

FIGURE 1 From a severity score to a decision

"Critical vulnerability. CVSS 9.8. Patch urgently."

HOW OFTEN

About once in 2 years

×

HOW MUCH

KES 2,000,000 a time

=

EXPECTED LOSS

About KES 1,000,000 a year

Illustrative numbers, using the FAIR approach: frequency multiplied by magnitude, in money [4].

A finding with a severity score asks for attention. A finding with a shilling figure asks for a decision.

03 The Kenyan specifics

Some of the numbers an owner cares about are set by law. Under Kenya's Data Protection Act, a data controller must notify the Data Commissioner of a personal data breach within seventy-two hours of becoming aware of it [5]. The administrative fine is capped at five million shillings or one per cent of the preceding year's turnover, whichever is lower [5]. For a large organisation that cap binds low, which means the bigger cost of a breach is often operational: downtime, recovery and members who quietly move their savings elsewhere. A defender who knows the business can say which of those dominates, and by roughly how much.

FIGURE 2 What Kenya's Data Protection Act sets

BREACH DISCOVERED

WITHIN 72 HOURS: NOTIFY THE DATA COMMISSIONER



Maximum fine: KES 5 million or 1% of the previous year's turnover, whichever is LOWER.

Sections 43 and 63 [5]. Not legal advice.

04 Month-end in Thika

ILLUSTRATIVE SCENE

An analyst at a savings co-operative wants to roll out multi-factor authentication for all staff and proposes the 28th, a quiet Saturday on the IT calendar. The manager refuses: the 28th is loan disbursement week, when salaries land and members queue at the counters. A second analyst, who knows the co-operative's calendar, proposes the 3rd instead, after the peak. She also prices one day of M-Pesa paybill downtime at the co-operative's scale, using the previous month's transaction volume, and uses that figure to argue for a backup connection. Both analysts are technically right about multi-factor authentication. Only one of them got it approved.

05 What OCH is building

OCH's coach is designed to keep asking the business question when learners practise: what would this cost the organisation, in shillings? Several drills already carry Kenyan data-protection and fraud scenarios. A fuller ladder of business-intimacy drills, from how a business makes money through to owner-level trade-offs, is in development rather than live, and this essay should not be read as claiming otherwise.

06 What would change our mind

If employers in the Kenyan market do not reward business translation when they hire or promote security staff, the career case in this essay weakens, even if the professional case stands. It is also possible that business understanding is learned faster on the job than before it, in which case training time is better spent on technical depth. Both are observable in placement and promotion outcomes, which OCH will collect as cohorts move into work.

07 What to do on Monday

For learners. Choose one business you know, a co-operative, a school or a shop, and write five lines on its cash, margin, velocity, growth and customers. Then estimate what one hour of its main system being down would cost, and write down how you got the number.

For mentors. When a learner presents a finding, ask them to restate it as a frequency and a cost before you discuss the fix.

For employers. Ask a candidate to explain one security risk to your finance manager in two minutes. You will learn more about how they will work with your business than any technical question will show.

REFERENCES

- [1] National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29. February 2024. Govern: Organizational Context (GV.OC).
- [2] UcedaVélez, T. and Morana, M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Wiley, 2015.
- [3] Charan, R. *What the CEO Wants You to Know*. Crown Business, 2001.
- [4] Freund, J. and Jones, J. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, 2014.
- [5] Republic of Kenya. *Data Protection Act No. 24 of 2019*, sections 43 and 63. Not legal advice.

Drafted with AI assistance and reviewed before publication. External figures were checked against the sources cited; scenes marked illustrative are composites, not reports of real events; OCH figures are dated.