AFRICA | NIL

THE COST OF A BREACH VS. THE COST OF TRAINING WHICH WOULD YOU CHOOSE?

In South Africa, a data breach can devastate a business. Training employees costs a fraction, and helps prevent costly incidents.

THE COST OF A BREACH (SOUTH AFRICA, 2025)

AVERAGE COST:
R44.1 million per incident

DETECTION & CONTAINMENT TIME:
~277 days

BUSINESS IMPACT:
Loss of customers and trust POPIA fines and legal exposure Downtime & lost revenue
Long-term reputational damage

SMB IMPACT:
Up to 60% of small businesses close within 6 months of a major breach

COST BREAKDOWN:

DETECTION & ESCALATION
R17,500,000

LOST BUSINESS
R13,100,000

POST-BREACH RESPONSE
R12,500,000

Notification costs
R950,000

TRAINING COSTS LESS THAN A BREACH

TRAINING COSTS

SECURITY AWARENESS TRAINING
R700–R1,800 per employee/year

TECHNICAL CERTIFICATIONS
R5,000–R90,000 (depending on vendor/programme)

Companies with trained staff report 70% fewer phishing incidents.

Every R1 spent on training can save up to R4 in avoided breach costs.

Strengthens compliance with POPIA and industry regulations.

QUICK COMPARE

BREACH	TRAINING
R44.5-million	R700 - R1,800 per employee per annum
277 days to detect	Ongoing, proactive defence
POPIA fines, legal costs, downtime	Stronger compliance and uptime
Loss of trust, reputational damage	Customer confidence and business resilience

THE CHOICE IS CLEAR: REACTIVE SPENDING AFTER A BREACH...
OR PROACTIVE INVESTMENT IN YOUR PEOPLE.
INVEST IN TRAINING TODAY. PROTECT YOUR TOMORROW.