COMELY GLOBAL INSURANCE AGENCY LTD

- Personal Finance & Business Solutions -

P.O. Box 37715 - 00100 Nairobi
+ 254 117 575 648 | +254 750 611 664
simon@comelyglobalconsulting.com
www.comelyglobalconsulting.com/

CYBER INSURANCE

Simon Muchiri
Licensed Insurance & Financial Advisor
+254 117 575 648 | +254 750 611 664
simon@comelyglobalconsulting.com
https://comelyglobalconsulting.com

Licensed by Insurance Regulatory Authority (IRA)

Table of Contents

EXECUTIVE SUMMARY

Your Challenge: Your business operates online—e-commerce, digital services, customer databases, M-Pesa transactions, online banking. Cybercriminals target Kenyan businesses daily: ransomware locks your systems demanding Ksh 5M, hackers steal 50,000 customer records, phishing scam wires Ksh 2.8M to fraudsters, website goes offline for 72 hours losing Ksh 1.2M in sales. One cyber-attack can bankrupt your business, destroy customer trust, trigger lawsuits, and violate data protection laws (fines up to Ksh 5M).

The Risk of Inaction: Ransomware encrypts all business data—you cannot operate for 3 weeks, lose Ksh 8M in revenue, pay Ksh 3M ransom (no guarantee data restored), spend Ksh 1.5M on IT recovery. Customer data breach—20,000 records stolen, GDPR/Kenya Data Protection fines Ksh 3M, customer lawsuits Ksh 6M, reputation destroyed. Without cyber insurance, you pay everything from working capital, possibly closing the business permanently.

The Solution: Cyber Insurance (Cyber Liability Insurance) providing comprehensive protection for digital businesses: ransomware payments and negotiation, data breach response and notification costs, business interruption from cyber-attacks, cyber extortion coverage, legal defense for data breach lawsuits, regulatory fines and penalties, PR crisis management, and IT forensics and system restoration.

Investment: Ksh 120,000 - 1,500,000 annually depending on annual revenue (typically Ksh 300K-600K for SMEs with Ksh 50M-200M turnover), data sensitivity, security measures, and coverage limits (Ksh 10M-50M).

Why Act Now:

- Cyber-attacks on Kenyan businesses up 67% in 2024
- Average cyber-attack cost: Ksh 4.5M (far exceeds premiums)
- Kenya Data Protection Act violations = fines up to Ksh 5M
- Customers demand proof of cyber security (insurance demonstrates commitment)
- One attack without insurance = business closure risk

THE PROBLEM: WHY CYBER INSURANCE IS CRITICAL FOR KENYAN BUSINESSES

The Explosive Growth of Cyber Crime in Kenya

Statistics:

- Cyber-attacks on Kenyan businesses: +67% increase vs 2023
- Average cost per cyber incident: Ksh 4.5M
- Ransomware attacks: +85% (most common threat)
- Data breaches affecting 10,000+ records: 47 incidents reported
- Business email compromise (BEC) average loss: Ksh 2.8M
- 73% of Kenyan SMEs have NO cyber security insurance

Why Kenya is Targeted:

- Rapid digital adoption (M-Pesa, e-commerce, mobile banking)
- Weak cyber security in many SMEs (easy targets)
- Limited cyber security awareness
- High-value targets (fintech, e-commerce with payment data)
- Cross-border criminals operating from abroad

Devastating Scenarios Without Cyber Insurance

Scenario 1: E-Commerce Business—Ransomware Attack

Business: Online fashion retailer selling clothes and accessories

- Annual revenue: Ksh 85M
- Customer database: 45,000 customers
- Platform: Custom website + M-Pesa/card payments
- Staff: 18 employees (warehouse, customer service, logistics)

The Attack (Monday 9am): Employee opens email attachment (fake invoice). Ransomware deploys across entire network within 2 hours. All systems encrypted: website offline, customer database locked, order management system inaccessible, accounting software encrypted, email down.

Ransom Demand: Ksh 4,500,000 in Bitcoin (72-hour deadline or data deleted permanently)

Immediate Impact:

- Website offline—cannot process orders (peak season, expecting Ksh 800K daily sales)
- Cannot fulfil existing orders—customer complaints escalate
- Cannot access customer contact info to communicate
- M-Pesa till down—no payment processing
- Staff idle (cannot work without systems)

Financial Losses:

- Lost sales (21 days downtime): Ksh 16,800,000
- Ransom payment (negotiated to Ksh 3.2M): Ksh 3,200,000
- IT forensics and recovery: Ksh 1,400,000
- New security systems: Ksh 850,000
- PR crisis management: Ksh 320,000
- Customer compensation (goodwill): Ksh 450,000
- Staff costs during downtime: Ksh 680,000
- **Total cost: Ksh 23,700,000**

Long-term damage:

- 35% customer loss (go to competitors during downtime)
- Reputation damaged ("insecure website")
- Revenue down 40% for 6 months post-recovery
- Staff morale devastated

Without Cyber Insurance:

- Business has Ksh 8M working capital
- Cannot absorb Ksh 23.7M loss
- Cannot pay ransom (negotiations fail, data lost)
- Must rebuild from scratch—takes 3+ months
- Loses peak season revenue
- Business closes within 6 months

With Cyber Insurance (Premium: Ksh 420,000/year, Ksh 25M coverage):

- Insurance provides 24/7 cyber incident hotline
- Ransomware negotiator appointed (brings ransom down from Ksh 4.5M to Ksh 3.2M)
- Insurance pays ransom: Ksh 3.2M
- IT forensics covered: Ksh 1.4M
- Business interruption coverage: Ksh 14M (lost revenue during downtime)
- PR firm hired to manage reputation: Ksh 320K
- New security systems funded: Ksh 850K
- **Total insurance payout: Ksh 19.77M**
- Business resumes operations day 8 (vs 60+ days without insurance)
- Customer trust restored through professional response
- Business survives and thrives

Scenario 2: Fintech Start-up: Data Breach

Business: Mobile lending app (personal loans via app)

- Annual revenue: Ksh 125M
- Customer base: 78,000 users
- Data held: Names, IDs, KRA PINs, bank details, M-Pesa numbers, salary info, locations
- Staff: 32 employees

The Breach: Hacker exploits vulnerability in mobile app. Downloads database containing 78,000 customer records. Posts sample of 5,000 records on dark web as proof, demands Ksh 8M or releases all data publicly.

Regulatory Nightmare:

- Kenya Data Protection Act violation (failed to secure personal data)
- Office of Data Protection Commissioner launches investigation
- Potential fine: Up to Ksh 5,000,000
- Mandatory data breach notification to all 78,000 customers

Customer Lawsuits:

- 847 customers file claims alleging:
    - Identity theft using stolen data
    - Fraudulent loans taken in their names
    - Harassment from loan sharks who bought data

    - Emotional distress
- Average claim: Ksh 150,000
- **Total claims: Ksh 127,050,000**

Financial Impact:

- Data breach notification (78,000 customers via SMS/email/letters): Ksh 950,000
- Call centre (handling 15,000+ customer calls): Ksh 680,000
- Credit monitoring for affected customers (1 year): Ksh 3,900,000
- Legal defense costs: Ksh 2,500,000
- Regulatory fine: Ksh 5,000,000
- Settlement of customer claims (negotiated): Ksh 18,000,000
- IT security overhaul: Ksh 2,800,000
- PR crisis management: Ksh 850,000
- Lost customers (60% churn): Revenue impact Ksh 75M annually
- **Total cost: Ksh 34,680,000** (excluding lost revenue)

Without Cyber Insurance:

- Start-up has Ksh 18M in funding/cash
- Ksh 34.68M cost bankrupts company immediately
- Investors refuse additional funding (reputational damage)
- Cannot pay customer settlements—lawsuits escalate
- Cannot pay regulatory fine—business license suspended
- Company closes, founders personally liable for some claims

With Cyber Insurance (Premium: Ksh 680,000/year, Ksh 40M coverage):

- Immediate breach response team activated (within 2 hours of discovery)
- Forensics identify breach source and secure systems: Ksh 1.2M (covered)
- Legal experts handle regulatory response: Ksh 2.5M (covered)
- Customer notification managed professionally: Ksh 950K (covered)
- Credit monitoring for customers: Ksh 3.9M (covered)
- Regulatory fine: Ksh 5M (covered)
- Customer claim settlements negotiated and paid: Ksh 18M (covered)
- PR firm limits reputational damage: Ksh 850K (covered)
- **Total insurance payout: Ksh 33.4M**
- Business survives regulatory scrutiny
- Customer trust partially restored through responsible response
- Company continues operations (though significantly impacted)

Scenario 3: Digital Marketing Agency—Business Email Compromise (BEC)

Business: Digital marketing and social media management agency

- Annual revenue: Ksh 48M
- Staff: 12 employees
- Clients: 35 businesses (manage their social media, ad campaigns, websites)
- Holding client funds: Ksh 8.5M in escrow (for ad spend, campaigns)

The Scam: Cybercriminals hack company email, monitor communications for 3 weeks. Identify that company is about to transfer Ksh 2.8M to Meta (Facebook/Instagram) for client ad campaigns.

The Attack: Friday 3pm: Fake email sent from CEO's account (compromised) to accounts person instructing "urgent" transfer of Ksh 2.8M to different bank account (criminal's account) "for new vendor payment, need by Monday." Looks legitimate (CEO's real email, mentions real client names).

Accounts person transfers Ksh 2.8M. Monday morning: Real CEO has no knowledge. Money gone—transferred to offshore account, cannot be recovered.

Financial Impact:

- Client funds stolen: Ksh 2,800,000
- Cannot fulfil client ad campaigns (clients furious)
- Must refund clients from own funds: Ksh 2,800,000
- Clients terminate contracts (lose Ksh 18M annual revenue)
- Legal costs defending negligence claims: Ksh 850,000
- IT security audit and upgrades: Ksh 420,000
- Lost revenue from terminated clients: Ksh 18M over 12 months
- Reputation damage prevents new client acquisition for 8+ months
- **Total cost: Ksh 6,870,000** (plus lost revenue)

Without Cyber Insurance:

- Agency has Ksh 3.5M cash reserves
- Must refund clients Ksh 2.8M (legal obligation—it was their money)
- Cannot afford to lose Ksh 2.8M + legal costs
- Founders must inject personal funds or face business closure
- Reputation destroyed—"they lost our money"
- Business survives barely but struggles for 2+ years

With Cyber Insurance (Premium: Ksh 285,000/year, Ksh 15M coverage):

- Cyber fraud coverage triggers
- Insurance pays stolen funds: Ksh 2.8M (clients refunded immediately)
- Forensic investigation: Ksh 380K (identifies breach, secures systems)
- Legal defense if clients sue: Ksh 850K (covered—no client lawsuits as funds restored quickly)
- PR management : Ksh 180K (manages client communications professionally)
- **Total insurance payout: Ksh 4.21M**
- Clients' funds restored within 2 weeks
- Contracts maintained (most clients stay due to professional response)
- Revenue protected
- Business survives with reputation intact

Kenya-Specific Cyber Threats

1. M-Pesa Fraud

- Fake M-Pesa payment notifications
- SIM swap attacks targeting business M-Pesa accounts
- Till/paybill number hijacking

2. Mobile Money Agent Attacks

- Agents with Ksh 2M-5M float targeted
- Sophisticated scams draining agent accounts

3. Phishing Targeting Kenyan Businesses

- Fake KRA emails (tax refunds, penalties)
- Fake bank notifications (account suspended)
- Fake supplier invoices (payment urgent)

4. Ransomware

- Increasingly targeting SMEs (perceived as easy targets with weak security)
- Kenyan businesses paying ransoms averaging Ksh 3.2M

THE SOLUTION: COMPREHENSIVE CYBER INSURANCE

Core Coverage Components

1. First-Party Coverages (Your Direct Losses)

Coverage	What It Covers	Typical Limit
Business Interruption	Lost revenue during system downtime from cyber attack	50-100% of policy limit
Cyber Extortion/Ransomware	Ransom payments + negotiator costs	Up to policy limit
Data Recovery/Restoration	IT forensics, system restoration, data recreation	Ksh 2M-10M
Crisis Management	PR firm, customer communications, reputation repair	Ksh 500K-2M
Fraud/Theft	Funds stolen via cyber fraud (BEC, phishing)	Up to policy limit

2. Third-Party Coverages (Your Liability to Others)

Coverage	What It Covers	Typical Limit
Data Breach Response	Customer notification costs, call centres, credit monitoring	Ksh 1M-5M
Legal Liability	Defense costs + damages for customer lawsuits	Up to policy limit
Regulatory Defense	Defense costs for Data Protection Commissioner investigations	Ksh 1M-5M
Regulatory Fines	Fines from Kenya DPA violations (where insurable)	Ksh 2M-5M
Media Liability	Defamation, copyright infringement from your digital content	Ksh 2M-10M

Coverage Tiers

Basic Cyber Coverage (Small Digital Businesses)

- Coverage limit: Ksh 10,000,000
- Business interruption: 30 days
- Ransomware: Ksh 2M
- Best for: Small e-commerce, consultants, small apps
- Premium: Ksh 120,000 - 200,000/year

Standard Cyber Coverage (Growing SMEs)

- Coverage limit: Ksh 25,000,000
- Business interruption: 60 days
- Ransomware: Ksh 5M
- Data breach response included
- Best for: Medium e-commerce, fintech startups, SaaS companies
- Premium: Ksh 300,000 - 500,000/year

Comprehensive Cyber Coverage (Established Digital Businesses)

- Coverage limit: Ksh 50,000,000
- Business interruption: 90 days
- Ransomware: Ksh 10M
- Full data breach + regulatory coverage
- Best for: Large e-commerce, financial services, large databases
- Premium: Ksh 600,000 - 1,200,000/year

OUR ROLE AS YOUR CYBER (SMEs & DIGITAL) INSURANCE ADVISOR

What We Do for You:

- Seek cover with your preferred insurer or recommend best fit insurer for your needs (if you have no one)
- Handle documentations and submission to insurer
- Secure best possible rates
- Obtain insurance policy on payment of premiums
- Reminder before policy expiration (no lapse)
- Re-compare providers yearly (rates change)
- Coordinate seamless renewal
- Guide you through claims process
- Ensure proper documentation
- Follow up with insurer
- Fight denied claims (appeal if wrongfully denied)

No Advisory Fees:

You pay nothing for my services - providers pay my commission. You pay the same premium direct or through me—but gain expert guidance, needs analysis, and claims advocacy.

REAL SUCCESS STORIES

Case 1: E-Commerce Ransomware—Insurance Saved Peak Season

Client: Nairobi Fashion House (online clothing retailer)
Coverage: Ksh 20M cyber policy, premium Ksh 380K/year

The Attack: Ransomware hit during Black Friday week (peak sales period). Systems encrypted, website offline. Ransom: Ksh 4.2M.

Insurance Response:

- 24/7 hotline contacted within 1 hour
- Ransomware negotiator assigned within 3 hours
- Negotiated ransom down to Ksh 2.9M
- Insurance paid ransom: Ksh 2.9M
- IT forensics and clean up: Ksh 980K (covered)
- Systems restored: Day 4
- Business interruption: Ksh 3.2M lost sales (covered)
- **Total payout: Ksh 7.08M**

Outcome: Missed 4 days of Black Friday but recovered quickly. Lost sales covered by business interruption. Customer data secured. Total cost if uninsured: Ksh 12M+ (ransom + IT + lost sales + reputation damage). Premium: Ksh 380K. ROI: 1,763%

Case 2: Fintech Data Breach—Regulatory Crisis Managed

Client: QuickLoan Kenya (mobile lending app)
Coverage: Ksh 40M cyber policy, premium Ksh 950K/year

The Breach: 62,000 customer records stolen (names, IDs, bank details). Hacker demanded Ksh 6M or would publish data.

Insurance Response:

- Breach response team activated immediately
- Data Protection Commissioner notified (legal requirement)
- Customer notification managed: Ksh 1.2M (covered)
- Legal defense for regulatory investigation: Ksh 1.8M (covered)
- Customer credit monitoring (1 year): Ksh 3.1M (covered)
- Extortion negotiation: Insurance refused payment (policy encourages reporting, not paying criminals)
- Regulatory fine: Ksh 3.5M (covered)
- Customer settlements: Ksh 8.2M (covered)
- PR crisis management: Ksh 650K (covered)
- **Total payout: Ksh 18.45M**

Outcome: Business survived regulatory scrutiny, maintained operating license, settled customer claims professionally. Without insurance: Ksh 18M+ cost would have bankrupted startup. Premium: Ksh 950K. One breach justified 19+ years of premiums.

Case 3: Agency BEC Fraud—Client Funds Restored

Client: Nairobi Digital Marketing Ltd
Coverage: Ksh 12M cyber policy, premium Ksh 195K/year

The Fraud: Business email compromise. Ksh 1.9M wired to fraudsters (thought it was legitimate supplier payment).

Insurance Response:

- Cyber fraud coverage triggered
- Forensic investigation: Ksh 280K (covered)
- Police report filed (supported by insurance legal team)
- Stolen funds reimbursed: Ksh 1.9M (covered)
- Client relationships maintained
- **Total payout: Ksh 2.18M**

Outcome: Clients never learned funds were at risk (restored within 2 weeks). Contracts maintained, revenue protected. Without insurance: Ksh 1.9M loss would have required founders' personal funds, reputation destroyed. Premium: Ksh 195K. ROI: 1,018%

CYBER INSURANCE VS IT SECURITY—COMPLEMENTARY NOT COMPETING

Both Are Essential

IT Security	Cyber Insurance
Preventative: Reduces likelihood of attacks	**Reactive:** Covers financial impact when attacks succeed
Firewalls, antivirus, encryption, training	Ransomware payments, legal costs, lost revenue
Cannot prevent 100% of attacks	Protects when prevention fails
Ongoing cost (monthly/annual)	Annual premium (fixed cost)

Key Point: Insurance does NOT replace IT security. Insurers require minimum security standards (antivirus, backups, employee training). However, even best security cannot prevent all attacks—insurance covers the gap.

COMMON MISTAKES & HOW WE AVOID THEM

Mistake 1: "We Have IT Support, Don't Need Insurance"

Reality: IT support prevents attacks. Insurance pays when attacks succeed (and they will—1 in 4 businesses face cyber incidents).

Solution: Have both. Insurance complements security, doesn't replace it.

Mistake 2: Thinking "We're Too Small to Be Targeted"

Reality: SMEs targeted MORE than large companies (weaker security, easier targets). 73% of cyber-attacks in Kenya target SMEs.

Solution: Size doesn't matter—if you have data/money online, you're a target.

Mistake 3: Assuming General Business Insurance Covers Cyber

Reality: Standard business insurance EXCLUDES cyber risks. You need specific cyber policy.

Solution: I verify your existing coverage and show exactly what's excluded.

Mistake 4: Inadequate Coverage Limits

Problem: Buying Ksh 5M coverage when data breach could cost Ksh 15M. Shortfall comes from business/personal funds.

Solution: I calculate realistic exposure based on your data, revenue, customer base.

Mistake 5: Not Reading Exclusions

Problem: Assuming everything cyber-related is covered. Policies exclude: Known vulnerabilities not patched, lack of basic security, employee theft.

Solution: I explain exclusions clearly and help you meet security requirements.

FREQUENTLY ASKED QUESTIONS

Q1: Does cyber insurance pay ransomware demands?
Yes, most policies cover ransom payments. Insurers often include negotiators who reduce demands by 40-60%. However, some policies encourage reporting to authorities rather than paying.

Q2: Will insurance cover us if we don't have basic security measures?
No. Insurers require minimum security: antivirus, firewalls, regular backups, employee training. Without these, claims can be denied.

Q3: What if we're attacked and can't prove when attack started?
Policies cover attacks discovered during policy period, even if they started before (if unknown to you). Honest disclosure during application is critical.

Q4: Does insurance cover fines from Kenya Data Protection Act violations?
Partially. Insurers cover defense costs and fines where legally insurable. Intentional violations or gross negligence typically excluded.

Q5: What if employee causes breach (lost laptop, clicked phishing link)?
Covered, provided you had basic security training. Intentional employee theft/sabotage excluded.

Q6: Can we get retroactive coverage for past breaches we just discovered?
No. Only breaches discovered during policy period covered. This is why buying NOW is critical—you may have ongoing breach you're unaware of.

Q7: How quickly are cyber incident response teams deployed?
24/7 hotlines answer within minutes. Incident response teams (forensics, legal, PR) typically engaged within 2-4 hours of notification.

Q8: What happens to premium if we make a claim?
Premium typically increases 20-40% at renewal after claim. However, without insurance, one claim could bankrupt you—premium increase is manageable vs catastrophic loss.

TAKE ACTION NOW

Why Delay Costs You

Every day without cyber insurance:

- Cyber criminals scanning for vulnerable businesses
- One ransomware attack = Ksh 3M-10M loss
- Data breach = Ksh 5M-30M (notification + legal + regulatory + settlements)
- Business email compromise = Ksh 1M-5M stolen funds
- Your business one phishing email away from crisis

Statistics: 1 in 4 Kenyan businesses will experience cyber incident in next 12 months. Average cost: Ksh 4.5M. Cyber insurance premium: Ksh 200K-600K. One incident justifies 8-23 years of premiums. Can you afford to self-insure?

Get Your Cyber Insurance Quote Now - Contact Me Today

Simon Muchiri – IRA Licensed Insurance & Financial Advisor
Comely Global Insurance Agency Ltd
Phone: +254 117 575 648 | +254 750 611 664
Email: simon@comelyglobalconsulting.com
Website: https://comelyglobalconsulting.com

Office Hours: Monday - Friday, 8:00 AM - 6:00 PM

Cyber Insurance: Cyber-attacks on Kenyan businesses up 67% in 2024. Average attack cost: Ksh 4.5M. Ransomware, data breaches, fraud targeting SMEs daily. Premium: 0.4%-0.8% of revenue. One attack without insurance = business closure risk. Protect your digital business now.

Disclaimer: *Illustrative purposes only. Actual terms determined by selected provider based on revenue, data types, security measures, customer database size, and industry. Simon Muchiri/Comely Global Insurance Agency Ltd acts as independent advisor. Commission paid by insurers at no extra cost to clients.*