12. Cyber Insurance

Overview

Cyber threats are the defining business risk of our generation. Every organisation that stores customer data, processes payments online, or relies on digital infrastructure is a potential target — and the financial consequences of a successful attack can be catastrophic. Our Cyber Insurance policy provides comprehensive first-party and third-party cover that activates the moment an incident is detected, giving you the financial resources and expert support to contain the damage, restore operations, and manage the regulatory and reputational fallout.

Our cyber policies cover a wide spectrum of digital risks, including ransomware attacks, data breaches, business email compromise, social engineering fraud, system outages caused by malicious actors, and regulatory fines arising from data protection violations under frameworks such as Kenya's Data Protection Act and the EU's GDPR. Critically, our policies include access to a 24/7 cyber incident response team — comprising forensic investigators, legal counsel, PR specialists, and IT recovery experts — who mobilise immediately when a breach occurs, minimising the window of exposure.

> ***It is not a question of whether your organisation will face a cyber threat — it is a question of whether you are financially prepared when it happens.***

Policy Options

34. **Breach Response & Recovery**

    Covers forensic investigation, system restoration, data recovery, and legal notification costs following a data breach — including the expense of notifying affected individuals and regulators.

35. **Ransomware & Extortion**

    Covers ransom payments, negotiation costs, and business income losses resulting from ransomware attacks or cyber extortion demands that disrupt your operations.

36. **Regulatory Fines & Liability**

    Covers fines and penalties imposed by data protection regulators, plus third-party liability claims from customers or partners whose data was compromised in a breach.