CYBER SECURITY MANAGEMENT AND AWARENESS FOR ORGANISATIONS COURSE

Introduction

Most breaches in African organisations start with a person, not a firewall: a clicked link, a reused password, an approved fraudulent invoice. This course is written for the managers who own that risk rather than for engineers who configure devices. Participants learn to assess their organisation's exposure, put policies and controls in place that staff will actually follow, run an awareness programme that changes behaviour, prepare an incident response plan, and report cyber risk to the board in business language. Participants leave with a risk register, an incident response runbook and a twelve-month awareness plan for their own organisation.

Course Objectives

- Assess your organisation's cyber risk exposure and prioritise it
- Apply a recognised framework such as ISO 27001 or the NIST Cybersecurity Framework at management level
- Write security policies staff can follow: access, passwords, devices, remote work
- Run a staff awareness programme, including phishing simulations
- Recognise and prevent social engineering, business email compromise and invoice fraud
- Manage third-party and supplier security risk
- Build and test an incident response and business continuity plan
- Meet the security obligations in data protection law
- Report cyber risk and readiness to executives and the board

Course Modules

> Module 1: The Threat Landscape in Practice

- How organisations are actually breached

P.O Box 7254- 01000
www.trustgatecorporateskills.co.ke
Location Thika & Nairobi

- Ransomware, business email compromise and invoice fraud
- Insider threat, negligence and departing staff
- Mobile money and payment system fraud
- Threats specific to the public sector, NGOs and SACCOs
- Sources of credible threat information

> Module 2: Governance and Risk Assessment
- Who owns cyber risk in an organisation
- ISO 27001 and the NIST Cybersecurity Framework at management level
- Identifying critical assets and crown jewels
- Risk scoring, appetite and treatment decisions
- Building and maintaining a cyber risk register
- Budgeting security by risk rather than by vendor pitch

> Module 3: Policies and Everyday Controls
- Access control and the principle of least privilege
- Password policy and multi-factor authentication
- Device, bring-your-own-device and remote working rules
- Email, internet and social media use
- Backup, patching and basic hygiene the manager must insist on
- Writing policy people read and apply

> Module 4: The Human Layer
- Why awareness training usually fails
- Designing a rolling awareness programme
- Running phishing simulations ethically
- Onboarding, role change and exit procedures
- Reporting culture and rewarding near-miss reports
- Measuring behaviour change, not attendance

> Module 5: Third Parties and the Supply Chain
- Security due diligence before signing a supplier
- Security clauses in contracts and service agreements
- Cloud services and shared responsibility
- Managing contractor and consultant access
- Monitoring and reviewing supplier security
- Responding when a supplier is breached

> Module 6: Incident Response and Continuity

- Detecting and classifying an incident
- The first hour: containment and decision making
- Incident roles, escalation and communication
- Reporting obligations to regulators and data subjects
- Backups, recovery and business continuity testing
- Post-incident review and lessons learned

> Module 7: Reporting, Compliance and the Board

- Security obligations under data protection law
- Translating technical risk into business language
- Metrics and dashboards executives actually use
- Preparing for audits and client security questionnaires
- Building the case for security investment
- A ninety-day improvement plan for your organisation