EXECUTIVE CYBER RESILIENCE PROGRAMME

A Board-Level Crisis Simulation for Financial Institutions

JUNE 23–24, 2026

THE SITUATION: Africa

In 2025, criminals bypassed security at West African institutions by posing as bank staff on phone calls. The voices were AI-generated, cloned from real employees. Silent theft. Millions lost. This is what the new generation of threats looks like. Nearly 70% of fraud attempts targeting African financial institutions now use AI-generated identities. Cybercrime losses across the continent surged from $192 million to $484 million in a single year. Recovering from a breach costs African financial institutions an average of $3.9 million, the highest of any sector on the continent, a figure established by the IBM Cost of a Data Breach Report 2025.

Evolving legislation means regulators have stopped asking politely. The Nigeria Data Protection Commission fined institutions ₦400 million, while Kenya allows fines up to 1% of annual turnover. The financial cost is recoverable. The reputational damage, the customer exodus, the media coverage, the loss of correspondent banking relationships, often is not.

Regulators are no longer writing to IT. They are naming board directors and C-suite executives personally.

Most boards found out too late.

WHAT THIS PROGRAMME IS

A two-half-day executive programme built specifically for Global South financial institutions. Not a conference. Not a lecture series.

Your board and C-suite operate from a private "Distributed Command Center" inside your own boardroom. You receive expert briefings and work through a live, escalating cyber crisis simulation. All internal deliberations remain entirely on your own channels - nothing leaves the room.

JUNE 23, 2026 | 7:00AM - 12:30PM
DAY 1 - THE FIDUCIARY SHIELD

Focus: Governance, board liability, and regulatory exposure. Expert briefings on the 2026–2027 threat landscape, cross-border data laws, and cyber-enabled financial crime. Culminates in a facilitated Board Charter Plenary.

JUNE 24, 2026 | 7:00AM - 1:00PM
DAY 2 - CYBER ATTACK SIMULATION

Focus: Live crisis decision-making under real pressure. Includes a live ethical hacking demonstration against banking defences and a 60-minute escalating simulation with timed injects - ransom countdowns, simulated media leaks, regulatory notifications.

WHAT YOUR TEAM LEAVES WITH

Day 1 deliverable: A Localized Board Risk Charter, your institution's risk tolerances, governance boundaries, and a legally defensible framework, in writing.

Day 2 deliverable: A "Kill Switch" Ransomware Decision Protocol, a codified matrix specifying who holds authority in a crisis and under what conditions.

Throughout: A cross-functional team 72-hour breach response playbook and a defensible record of executive preparedness for regulators.

WHO SHOULD ATTEND

Board Chairman and Directors • Chief Executive Officer (CEO)

Chief Financial Officer (CFO) • General Counsel

Chief Risk Officer (CRO) • Chief Technology Officer (CTO)

Chief Compliance Officer (CCO) • Head of Corporate Communications

Chief Information Security Officer (CISO)

Your CISO already knows what's coming. This programme gets every other decision-maker in your institution on the same page, before the ransom clock starts.

GLOBAL SOUTH CYBERSECURITY & DATA PRIVACY SUMMIT 2026

WHAT ATTENDEES SAID

"The cross-section of panellists and the information they provided was excellent." ***- Jason Lewis, National Commercial Bank Jamaica***

"The relevance to our organisation was a 10 out of 10." ***- Daniel R. Reid, Cayman Islands Stock Exchange***

"The live simulation provided a realistic environment to stress-test our governance frameworks." ***- Summit Attendee***

GS-CDP SUMMIT FEBRUARY 2026 POST EVENT SURVEY

(Scored out of 10)

8.8 - **NPS score**

8.8 - **Relevance to their organisation**

8.7 - **Will apply learning within 90 days**

RETURN ON INVESTMENT

1. Regulatory exposure: Kenya's Data Protection Act allows fines of up to 1% of annual global turnover for non-compliance. For a mid-sized bank, that is a multi-million dollar liability.

2. Personal liability: Regulators are now holding board members and C-suite executives individually accountable for governance failures, not just the institution. Directors face personal fines, disqualification, and in severe cases, criminal exposure.

3. Reputational protection: A breach does not end when systems are restored. Customer trust, media coverage, and correspondent banking relationships take years to rebuild, if they rebuild at all. This programme equips your communications leadership to manage the narrative from the first hour.

4. Cost comparison: Custom tabletop exercises from international consultancies typically cost upwards of $50,000 USD. This programme trains up to 10 of your executives for $9,500 USD, $950 per decision-maker.

5. Operational protection: The average cost of a ransomware attack on an African financial institution is approx. $3.9M USD in recovery, lost business, and regulatory response. This programme costs less than 0.4% of that exposure.

GSPEN DTI HUB

EXECUTIVE CYBER RESILIENCE PROGRAMME

JUNE 23-24, 2026

The Expert Faculty

Global South experts in cybersecurity, law, risk and crisis management

June 23: The Fiduciary Shield | **June 24:** Cyber Attack Simulation

Jason Lau

Role: The Strategist

Programme Focus:
AI Predictions & Strategic Risk

Over 25 years of cybersecurity leadership experience shaping global security and privacy programmes. He secures digital assets for over 180 million users at one of the world's largest financial platforms. A Forbes Technology Council member, World Economic Forum contributor, and ISACA global board director, he is an award-winning leader who shapes global AI, privacy, and regulatory policy. He is recognized internationally for translating advanced threat intelligence into boardroom-ready strategy and delivers the 2026-2027 forward threat assessment, with a particular focus on AI-driven attacks now targeting regional financial data.

Niel Harper

Role: The Governor

Programme Focus:
ESG, Board Liability, & Risk Appetite

Over 20 years of experience advising global organizations on cybersecurity, enterprise risk, and board liability. A World Economic Forum Young Global Leader and ISACA Vice-Chair, he is one of the most credentialed cybersecurity governance voices in the Global South. He holds an LLM in Internet Law, making him one of very few cybersecurity executives with formal legal qualifications. He anchors the programme's governance and board liability curriculum across both days.

Rory Ebanks

Role: The Defender

Programme Focus:
Technical Incident Response & Forensics

Over 14 years of elite cybersecurity experience carrying CCISO, CEH, and CISSP credentials, the highest-level practitioner certifications in the field. He is the Caribbean's most recognized specialist in digital forensics, ransomware mitigation, and live incident response. Regularly engaged by Caribbean financial institutions to investigate and contain active breaches, he has trained hundreds of security professionals across the region. He delivers the Day 2 live deconstruction of a real regional bank hack.

Nyron Davidson

Role: The Auditor/ The Risk Manager

Programme Focus:
Financial Crime, Fraud, & AML/ CFT Compliance

Over 25 years of experience combating financial crime and leading compliance at the highest levels of global banking. A former United States Treasury Advisor and veteran Big 4 firm leader, he was the Head of Compliance Risk Management at a major financial institution. He guides global banks and fintechs on AML/CFT controls and complex fraud risk mitigation. He brings the auditor's lens your board needs: what regulators are actually looking for after a breach.

Rosalind Lake

Role: The Counsel

Programme Focus:
Cross Border Law

Over 20 years of legal experience as a premier authority on global cybersecurity and data privacy law at one of the world's leading international law firms. She guides multinational corporations through data sovereignty frameworks, AI governance obligations, and regulatory enforcement proceedings across multiple jurisdictions. A specialist in mandatory breach notification requirements and the financial implications of non-compliance for global enterprises, she transforms complex cross-border legal exposure into defensible corporate governance strategy. She leads the programme's session on navigating the financial and legal realities of international data privacy law.

Grace Lindo

Role: The Counsel

Programme Focus:
Legal Privilege, Fines

Over 15 years of experience as a leading authority on technology law, intellectual property, and corporate governance in the Caribbean. A Certified Information Privacy Professional, she navigates boards through the severe legal consequences of cyber breaches and regulatory investigations. She is an expert in legal privilege protections that shield board communications and co-leads the session on the legalities of the ransomware dilemma.

Deborah Hileman

Role: Communicator

Programme Focus:
Crisis Communication

Over 35 years of strategic crisis communication expertise across financial services, healthcare, and government sectors. A FEMA-trained Incident Command System commander, she is equipped to the same standard as federal emergency responders. She is internationally recognized for her work at the intersection of reputational risk and board accountability. She leads the crisis communications module, including drafting critical public statements under pressure.

Dr. Bright Gameli Mawudor

Role: Ethical Hacker

Programme Focus:
Ethical Hacker

Over 14 years of professional cybersecurity expertise as a pioneering ethical hacker and global strategist. Holding a PhD in Information Security, he was recognized in the Top 40 Under 40 in African technology and founded AfricaHackon. He advises government agencies and boards on systemic vulnerabilities in critical financial infrastructure. He delivers the live ethical hacking demonstration, revealing how AI-driven attacks bypass modern banking defenses.

EXECUTIVE CYBER RESILIENCE PROGRAMME

A Board-Level Crisis Simulation for Financial Institutions

JUNE 23–24, 2026

Programme Fee

Early booking deadline: April 30, 2026

Tier 1 Institutions

(Designed for larger, multi-jurisdictional banks, insurers, and conglomerates, with greater than 500 employees)

Team Size	Early Booking Advantage ($USD)	Standard Booking ($USD)
Full secure access for an Executive Team of **up to 10 persons.**	**$7,600** (save $1900)	**$9,500**

Tier 2 Institutions

(Designed for regional banks, credit unions, and scaling fintechs, with less than 500 employees)

Team Size	Early Booking Advantage ($USD)	Standard Booking ($USD)
Full secure access for an Executive Team of **up to 5 persons.**	**$3,800** (save $950)	**$4,750**

Introductory Executive Programme Pricing - offered at this rate because we believe every financial institution in the region should have access to this level of governance preparedness. At $950 per executive, this is the most cost-effective board-level cyber governance investment available. This rate will be increased for subsequent editions.

Need a larger team? Additional access seats beyond the included limit (10 for Tier 1; 5 for Tier 2) is available for USD $950 per person.

Common Questions From Boards

Is our internal data and discussion secure?

Yes. Your team operates entirely on your own internal channels. You stream our expert briefings, but all deliberations, risk assessments, and votes happen privately. Nothing leaves your boardroom.

Will we just be listening to presentations?

No. Day 1 produces a working Board Risk Charter before you close. Day 2 puts your team through a live, escalating attack simulation with timed injects — ticking countdowns, simulated media leaks — that force real decisions in your private war room.

What do we leave with?

Two working documents: a Localized Board Risk Charter (Day 1) and a codified Kill Switch Ransomware Decision Protocol (Day 2). These are usable governance tools — not a certificate or a slide deck.

Who should attend from our institution?

Board Members, CEO, CFO, General Counsel, Chief Risk Officer, Head of Corporate Communications, and the CISO. Cross-functional participation is essential — the programme is designed for the whole decision-making team, not just IT leadership.

EXECUTIVE CYBER RESILIENCE PROGRAMME - JUNE 23-24, 2026

$3.9M (USD) (Average ransomeware recovery cost) | **$950** (USD) (per executive in this programme)

Bring your entire decision-making team.

Global capacity: 65 institutions. Registration is open. Secure your team's early rate before capacity is reached.

To register or make an enquiry: forward this document to your Executive Assistant and copy sales@gspen.net - our concierge team will handle all onboarding, confirmation, and pre-programme coordination directly with them on your behalf.

Early booking Advantage closes once capacity is reached or on Thursday 30, April 2026 - whichever comes first.

After that date, the early rate becomes the standard rate and places are not guaranteed.

Contact: www.gspen.net | sales@gspen.net

Brought to you by GSPEN DTI HUB