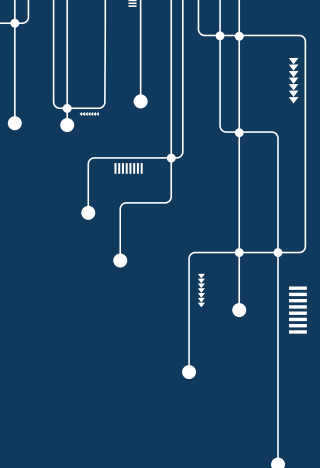




Cyber Security:

Building Resilient, Trusted Pension Systems

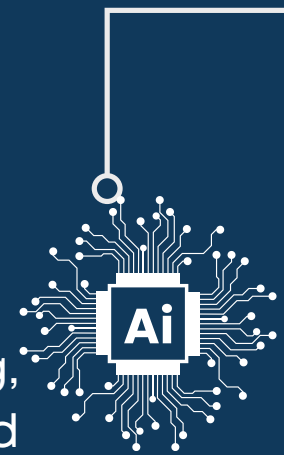
Who am I?

- Offensive Security Researcher: I love everything **Hacking**
- **Tribe of Hackers**: Blue Team 2020
- **Global Advisory Board**:
 - EC-Council for **C|TIA & C|PEN**
 - USIU-A ICT & Board Council
 - Ushahidi
 - CyberSafe Foundation
- Blockchain/Crypto Investigator
- Senior Technology Advisor to the **Attorney General of Kenya**
- **C.E.O Cyber Guard Africa**
- **Founder** of Cyber Collective, **Africahackon**
- Presented at over 449 Cyber Security conferences
- **Adjunct Professor**, Cyber Security - **Strathmore University**
- Practice Kung Fu



The Emerging Crime Map for Pension Industry

- **AI-enabled social engineering and deepfake fraud**
Synthetic voice and video used to authorise payments, resets and disclosures. **ACTIVE**
- **Identity and SIM-linked account takeover**
The mobile identity as a single point of failure for everything attached to it. **ACTIVE**
- **Third-party and supply chain compromise (API Security Exposure)**
The weakest vendor becomes the shortest route in, and inherits our trust. **ACTIVE**
- **Ransomware and extortion-as-a-service**
Encryption is now secondary. The real leverage is disclosure and regulatory exposure with actual confirmed data **ACTIVE**
- **Harvest-now, decrypt-later data theft**
Encrypted data taken today against decryption capability expected tomorrow. **EMERGING**



The line between real and artificial is blurring, bringing with it new risks, new deception tactics, and new levels of urgency for cybersecurity.

Passive Country Wide Research of Kenya

100,000+ IP Addresses in the country

3728 API Endpoints

1,279- Total Findings

592 - Critical Vulnerabilities

4.8M - Leaked Credentials

All activities were passive

1

APPLICATIONS
that deliver the outcomes you want

2

DATA
compliant, protected, accessible,
backed up

3

USERS
an engaging experience everywhere
they work

4

CUSTOMERS
a differentiating experience across
every channel

5

THINGS
connected to realise your IoT
strategy

Cyber Security vs Resilience

Cyber Security is Dead.

We have to start thinking about **CYBER RESILIENCE**

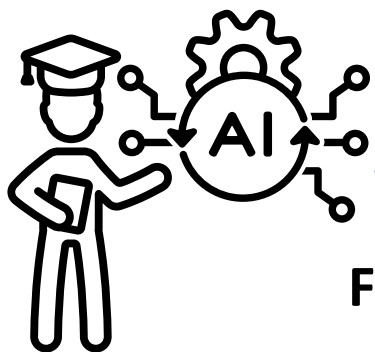
Cyber Security = Prevention and protection

Cyber Resilience = Ability to prepare for, withstand, recover from, and adapt to cyber incidents

The Four Pillars of Cyber Resilience:

1. **Anticipate:** Threat intelligence, scenario planning, red team exercises
2. **Withstand:** Defense in depth, zero trust architecture, segmentation
3. **Recover:** Incident response, business continuity, disaster recovery
4. **Adapt:** Lessons learned, continuous improvement, evolving controls





Artificial Intelligence Removed Three Barriers

For **thirty years**, three things limited who could commit a technology crime. Between 2023 and today, all three were removed.

01

Skill

Capability that once took years to develop is now rented by the month. The attacker no longer needs to understand the attack they are running.

02

Language

Fluent, contextually correct English and Swahili at volume, with no human writer. The spelling errors we taught staff to look for are gone.

03

Cost

A convincing synthetic voice costs less than lunch. Targets that were previously not worth the effort are now worth automating.

The consequence: Attack volume is rising while cost per attempt falls and quality is rising at the same time. The two used to trade off against each other. They no longer do.

AI-Enabled Fraud & Social Engineering: The New Threat Vector

Generative AI has fundamentally lowered the skill threshold for sophisticated fraud - what required a nation-state in 2020 can now be executed by a criminal group with \$500 and an API key.

AI-Enabled Attack Vectors



Executive Deepfake Voice/Video

Attackers clone CFO/CEO voice (30 seconds of audio needed) and call finance teams to authorise wire transfers. Already used against African banks in 2024.



AI-Personalised Phishing (Spear Phishing 2.0)

GenAI scrapes LinkedIn, company websites, regulatory filings to craft hyper-personalised emails. The company pension statements, transaction confirmations, and member communications are ideal lure templates.



Synthetic Identity for KYC Bypass

AI-generated faces + forged documents pass basic biometric KYC checks. Targeted at new account opening for pension benefits and property transactions. High payout targets.



Document Forgery at Scale

AI generates convincing title deeds, pension benefit statements, court orders. The company's property arm is directly exposed - due diligence processes must be updated for AI-era document verification.

Defensive Responses

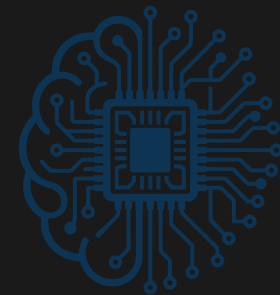
- Multi-party approval (MPA) for all transactions above defined thresholds - no single authoriser
- Call-back verification protocol: all CEO/CFO wire transfer instructions confirmed via pre-registered callback number
- AI deepfake detection tooling at video conferencing layer
- Liveness detection + document authenticity AI integrated into KYC pipeline
- Staff awareness: 'When in doubt, stop and call' - no urgency pressure accepted
- Fraud hotline with direct CISO escalation path
- Regular red team exercises specifically simulating AI-assisted social engineering
- AI-generated content watermarking policy for internal document workflows

Shadow AI: You Are Already Exposed



**“Your company is already using AI you don’t control.
And no one is accountable for it.”**

- Inga Stirbyte



LETS REMEMBER: THE ATTACKER IS RUNNING A BUSINESS



How they are pictured

- A lone opportunist
- Technically exceptional
- Motivated by notoriety
- Selects targets at random
- A technology problem

How they are Actually Operate

- A distributed organisation with specialist roles
- Buys capability rather than building it
- Motivated by return on invested effort
- Selects targets on expected yield
- A commercial problem with a technical surface



**You do not defeat a rational commercial actor.
You make yourself the more expensive target.**

WHERE DOES THE EXPOSURE SIT

Honest position:

NO product on the market today would have prevented this.

01

People: Dominant failure point

Awareness training does not survive the combination of authority, urgency and a familiar voice. Assume the training will fail and design for it.

02

Process: Where the fix mostly lives

Verification standards, authorisation thresholds, out-of-band confirmation, and the question of what any single individual can approve on their own.

03

Technology: Necessary, not sufficient

Controls see nothing when the credentials are valid, the request is well-formed and the voice sounds correct. Detection must shift to behaviour and anomaly.

04

Review

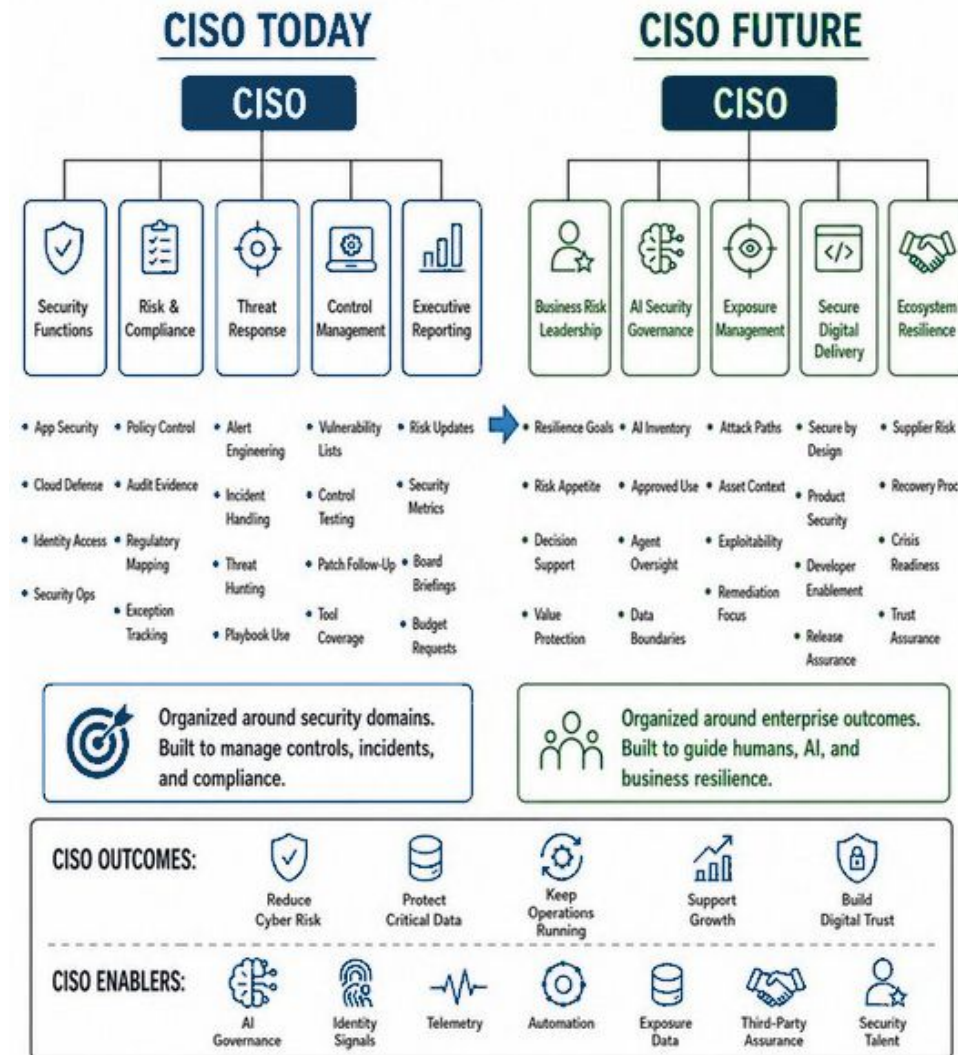
You can have all the above 3 points but without constant review, they are pointless.

A MATURE CISO SHOULD BE ABLE TO ANSWER THREE QUESTIONS CLEARLY

- What business outcome are we protecting?
- What level of risk are we accepting?
- How does this security investment improve resilience or decision-making?

CISO TODAY VS FUTURE

How the security leader role is shifting from function control to business resilience
by Excellog.Biz



© Excellog.Biz

Follow us for more like this



Five questions YOU should ask, every Quarter

- 1 Can we detect an identity-based compromise in which no malware is ever used? Show us the evidence, not the policy.
- 2 How long from compromise to detection to containment? Give us the trend across quarters, not a single figure.
- 3 What can one convinced employee authorise on their own: across voice, digital and agent channels?
- 4 What proportion of our critical third parties have we actually tested, as opposed to surveyed by questionnaire?
- 5 When did we last rehearse this live, under pressure, rather than on paper?

Build an Environment to Support Threat Hunting



Know Yourself

- Knowing your environment better than any INSIDER THREAT or EXTERNAL THREAT actors.
- If you REALLY want to protect your environment, you REALLY have to know your environment better than anyone.



Know Your Enemy

- Define your enemies, are they internal, external or both
- What is their capability? What motivates them?, What do they target?



Know your Battles

- Why will they target us? How can they impact our vision, mission?
- What will they target ? What are our crown jewels?
- How will they target? Have we seen attempts before?
- Where are we exposed? How does our attack surface reflect?

Design

Re-design

Implement

Operate

Monitoring

**D
R
I
O
M**



1. Discover & Assess

- Identify requirements, business & regulatory – i.e. HIPAA, PCI, SOX, GDPR, etc. Leverage BCP & GRC documentation
- Identify assets in scope and crown jewels
- Understand business and risk appetite
- Identify resources available: tools, budget, personnel, skills, time
- Practical threat modeling and risk analysis
- Attack surface analysis, network attack surface, data egress analysis, network visibility analysis and protocol visibility analysis
- Red teaming: impact analysis (think offensive), realistic scenarios based on attacker's TTP's

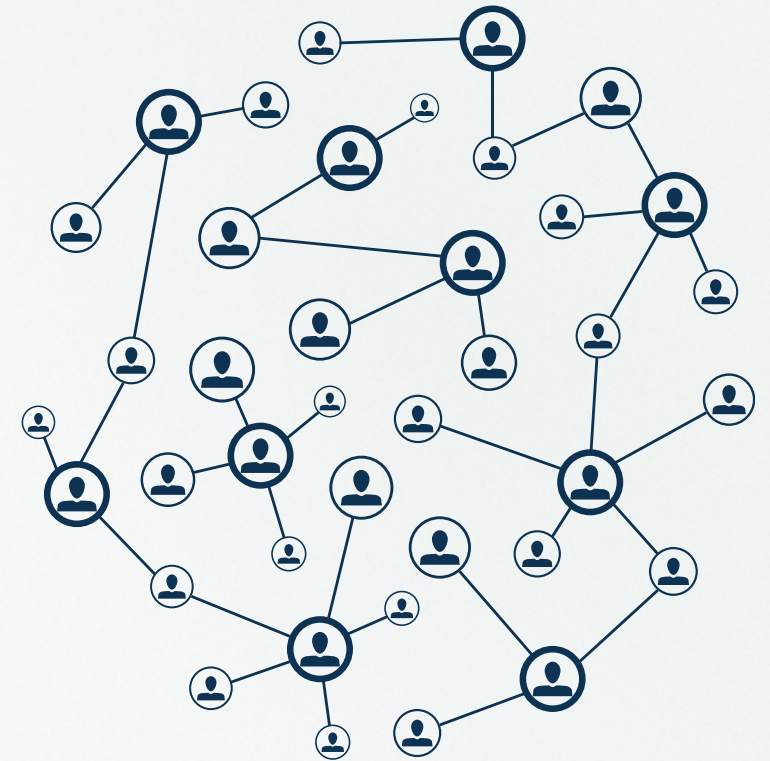


2. Re-Design

- Identify desired state, determine the gap (current vs. desired) and roadmap
- Architectural decisions
- Threat focused, covering protection, detection and reaction
- Risk mitigation
 - People
 - Processes
 - Technology
 - Controls
- Documentation

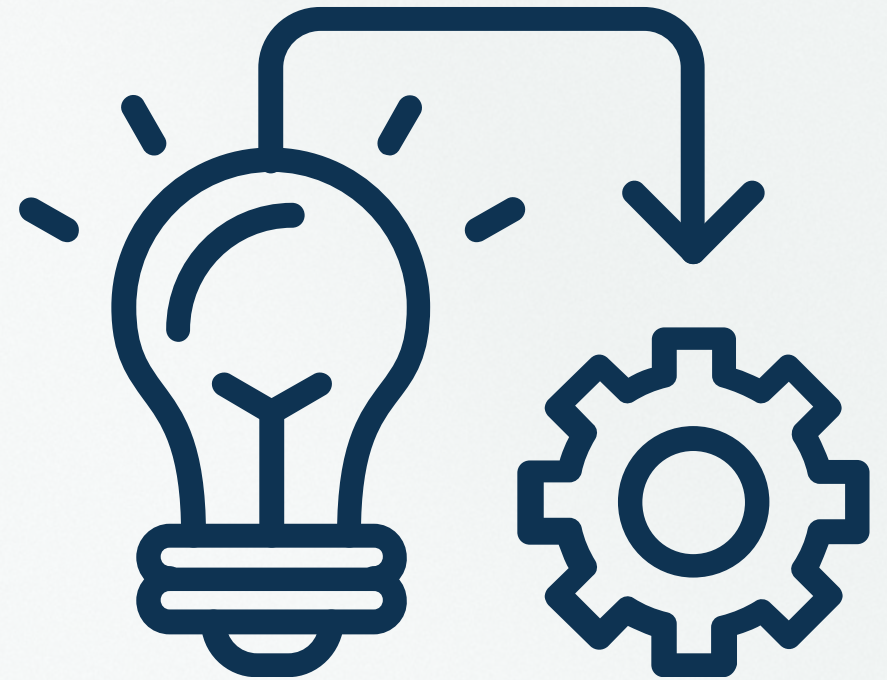
Some of the documentation needed here is:

 - Business rules regarding the handling of data/information assets
 - Written and published security policy
 - Codified data/information asset ownership and custody
 - Risk analysis documentation
 - Data classification policy documentation



3. Implement

- Implement based on security architecture design
- Harden at each layer
- Network-centric
- Data-centric
- Enable logging for monitoring
- Determine baseline
- Device configurations and traffic flows
- Validate implementation



4. Operate & Monitor

- Continuous security monitoring
- Data at rest: registry keys, windows event logs, DNS, etc.
- Network Security Monitoring
- Data in motion: NetFlow, transactional, pcaps
- Continue creating awareness, maintaining threat focused operations and augmenting visibility based on threat intel and IR lessons learned



Moving on with Business

Automating the onboarding and reassessment workflow to enable quicker, more flexible risk mitigation

Gaining deeper visibility into risk exposure across both third- and fourth-party relationships

Identifying non-compliant vendors and offboarding them in a way that maintains uninterrupted business operations

Expediting due diligence and risk evaluations to thoroughly vet vendors prior to onboarding

Implementing continuous monitoring through real-time data inputs and analytics

Refining security requirements in response to newly detected threats and vulnerabilities

Reducing Risk & Managing Incidents

1. Implement Zero Trust Security

- Traditional perimeter-based security is no longer sufficient.
- A Zero Trust model, which assumes that no user or device is trustworthy by default, helps minimize attack surfaces. Implementing multi-factor authentication (MFA), least privilege access, and continuous monitoring can prevent unauthorized access.

2. Regular Backups and Recovery Planning

- Organizations should maintain offline, immutable backups that cannot be altered by attackers.
- Having a tested incident response plan ensures a quicker recovery without needing to pay the ransom.

3. Frequent & Practical Employee Awareness Training

- Many ransomware attacks start with phishing emails that trick employees into clicking malicious links.
- Regular cybersecurity training can help employees recognize threats and reduce the chances of an attack succeeding.

What should we ask the Board to approve

1

An annual board-level threat simulation

Run live, with directors participating rather than observing. Paper exercises do not test judgement under pressure.

2

An independent assessment of identity and authorisation controls

Covering voice, digital and agent channels together, since attackers move between them and our assurance currently does not.

3

Quarterly detection and containment reporting to the Risk Committee

Time-based metrics with trend, owned by management and tabled as a standing item.

4

Train all department and make customers aware with practicality when it comes to Incident Response

Internal tribes need to be cyber aware of emerging threats and customers need to understand these are the new ways they need to be secure as well as respond to individual incidents.

The question is no longer whether we are targeted, but whether we notice in time.



THANK YOU



WWW.CYBERGUARDAFRICA.COM
BRIGHT.GAMELI@CYBERGUARDAFRICA.COM
+254712421951