Cyber Interactive

Interactive Defense, Proactive Security.

Enwealth

For a better tomorrow

Safeguarding Pension Funds in the Digital Age:

Cybersecurity, Risk Management & Compliance Strategies

Trainer Profile

Kelvin Saitoti

- I deliver cybersecurity and Risk Management strategies to protect data, minimize risks, and ensure compliance while Empowering Organization to execute Business Strategies safely.
- Masters in Cybersecurity | CND |CEH | CompTIA Pentest+| CompTia Sec+ 501| ISO 27001 Lead Implementer| CCISO | CISSP | | Data Privacy | 11+ Years

- Mobile No: +254 701 213 240 / +254 782 966 418
- LinkedIn Profile: KELVIN SAITOTI

“What Would You Do?”

Imagine you receive an email from your pension administrator asking you to update your account details immediately due to a ***"security breach”***

What’s your next step?

Cyber Interactive
Interactive Defense, Proactive Security.

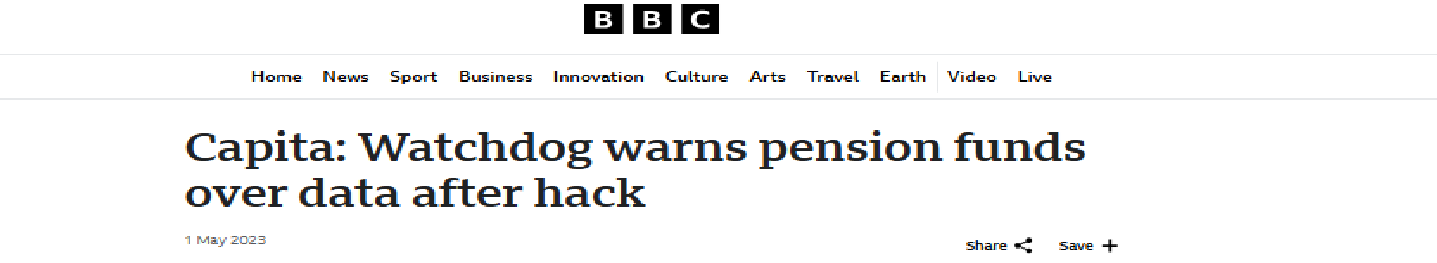
Welcome to this presentation on cybersecurity threats risk management and compliance strategies in Kenyan pension schemes. We will explore the evolving landscape of digital risks, examining statistics, and strategies for mitigation.

The goal is to provide you with **actionable** insights to safeguard your schemes and ensure the financial security of your members.

News

INTERPOL and AFRIPOL Arrest 24 Kenyans Involved in Online Credit Card Fraud Linked to a Loss of Ksh1.11 Billion. The Individuals Had Transferred the Stolen Funds to Companies in the UAE, Nigeria, and China Before Moving Them

27th November 2024



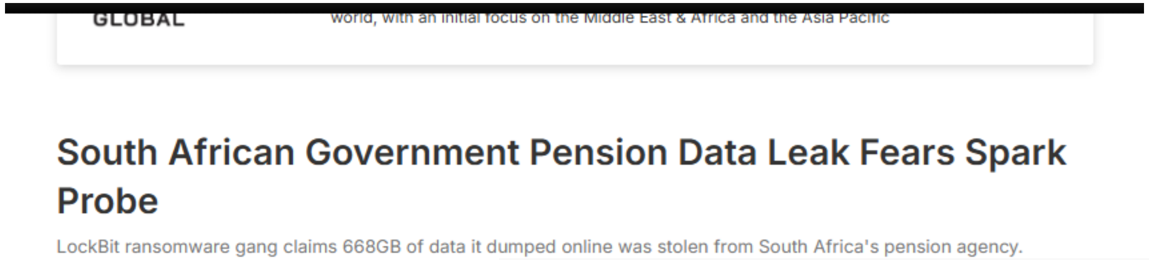
BBC

Home News Sport Business Innovation Culture Arts Travel Earth Video Live

Capita: Watchdog warns pension funds over data after hack

1 May 2023

Share Save +



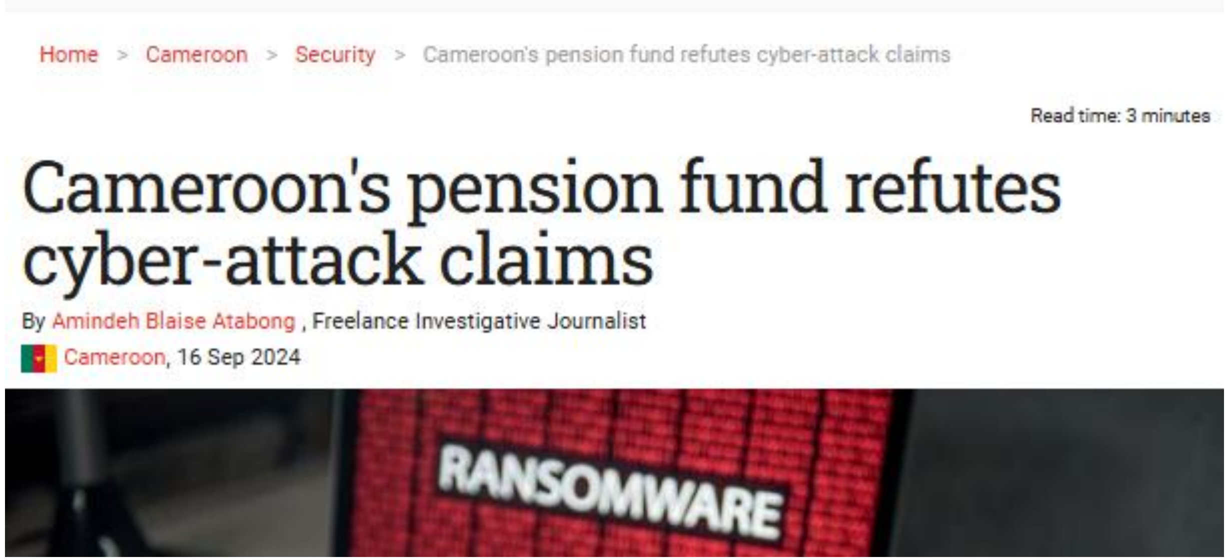
GLOBAL world, with an initial focus on the Middle East & Africa and the Asia Pacific

South African Government Pension Data Leak Fears Spark Probe

LockBit ransomware gang claims 668GB of data it dumped online was stolen from South Africa's pension agency.

John Leyden, Contributing Writer

March 18, 2024



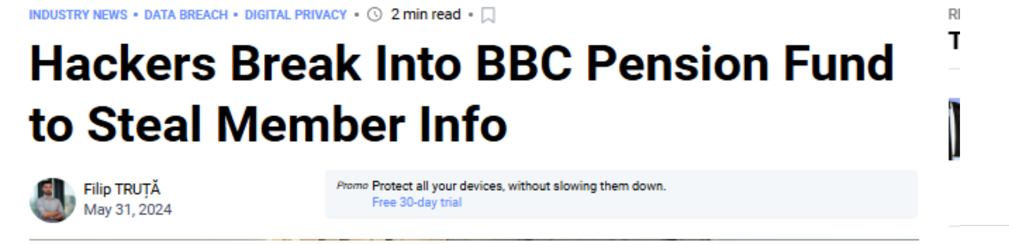
Home > Cameroon > Security > Cameroon's pension fund refutes cyber-attack claims

Read time: 3 minutes

Cameroon's pension fund refutes cyber-attack claims

By Amindeh Blaise Atabong , Freelance Investigative Journalist

Cameroon, 16 Sep 2024



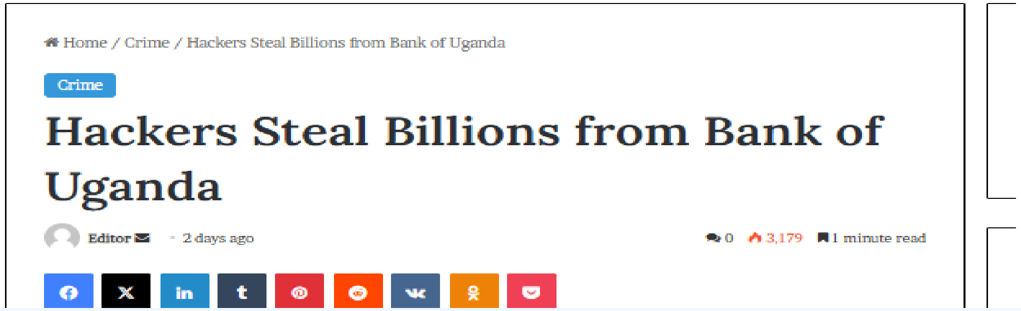
INDUSTRY NEWS • DATA BREACH • DIGITAL PRIVACY • 2 min read •

Hackers Break Into BBC Pension Fund to Steal Member Info

Filip TRUȚĂ

May 31, 2024

Promo Protect all your devices, without slowing them down.
Free 30-day trial

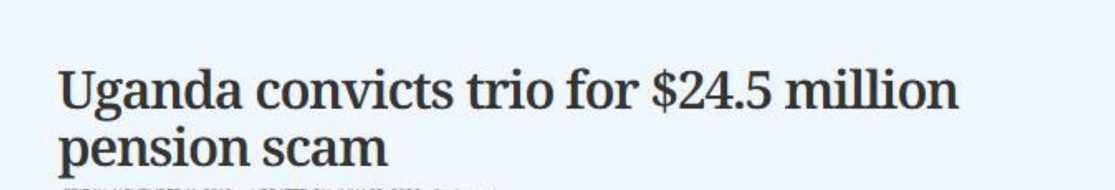


Home / Crime / Hackers Steal Billions from Bank of Uganda

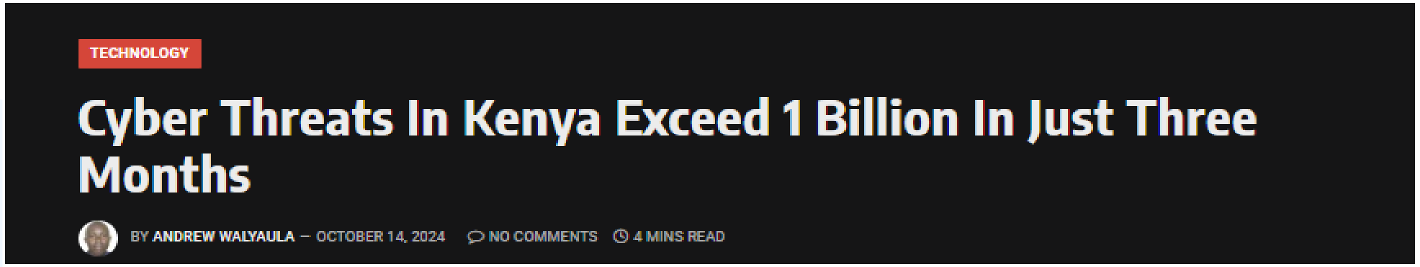
Crime

Hackers Steal Billions from Bank of Uganda

Editor · 2 days ago 0 3,179 1 minute read



Uganda convicts trio for $24.5 million pension scam



TECHNOLOGY

Cyber Threats In Kenya Exceed 1 Billion In Just Three Months

BY ANDREW WALYAULA — OCTOBER 14, 2024 NO COMMENTS 4 MINS READ

1.Evolving Threat Landscape

2. Understanding Attack Ecosystem

3.Focus Areas

4. Next Steps

OPERATION SERENGETI

Empowering Law Enforcement and Partners to Disrupt Cybercrime Networks Across Africa

INTERPOL

AFRIPOL

1,006 Arrests

Victims **35,224**

134,089 Malicious Network Takedowns

Pieces of Data Exchanged Via INTERPOL **6,703**

$192,976,558 Monetary Value Loss (USD)

Monetary Value Recovered (USD) **$43,964,537**

65 Cyber Activity Reports Disseminated

Participating Countries **19**

7 Private Sector Partners

Global Action on Cybercrime Enhanced - GLACY-e

Co-funded by the European Union

Co-funded and implemented by the Council of Europe

Federal Foreign Office

ISPA

WWW.INTERPOL.INT

AFJOC

Foreign, Commonwealth & Development Office

Cyber Interactive
Interactive Defense, Proactive Security.

The Rising Tide of Cyber Threats: A Statistical Overview

Breaches take a median length of **86 days** to be detected,
and **111 days** from intrusion to containment

27% of organizations encountered a **CEO fraud attack** in the past **12 months.**

74% of cybersecurity professionals say their organization has been impacted by the global cybersecurity skills shortage.

Through what avenue do you think your organization is most likely to get a system attacks ?

- **75%** – Email attachments
- **36.11%** – Malicious pop-ups or websites
- **19.44%** – Unpatched/vulnerable software programs
- **6.94%** – Removable media

Quote from the poll:

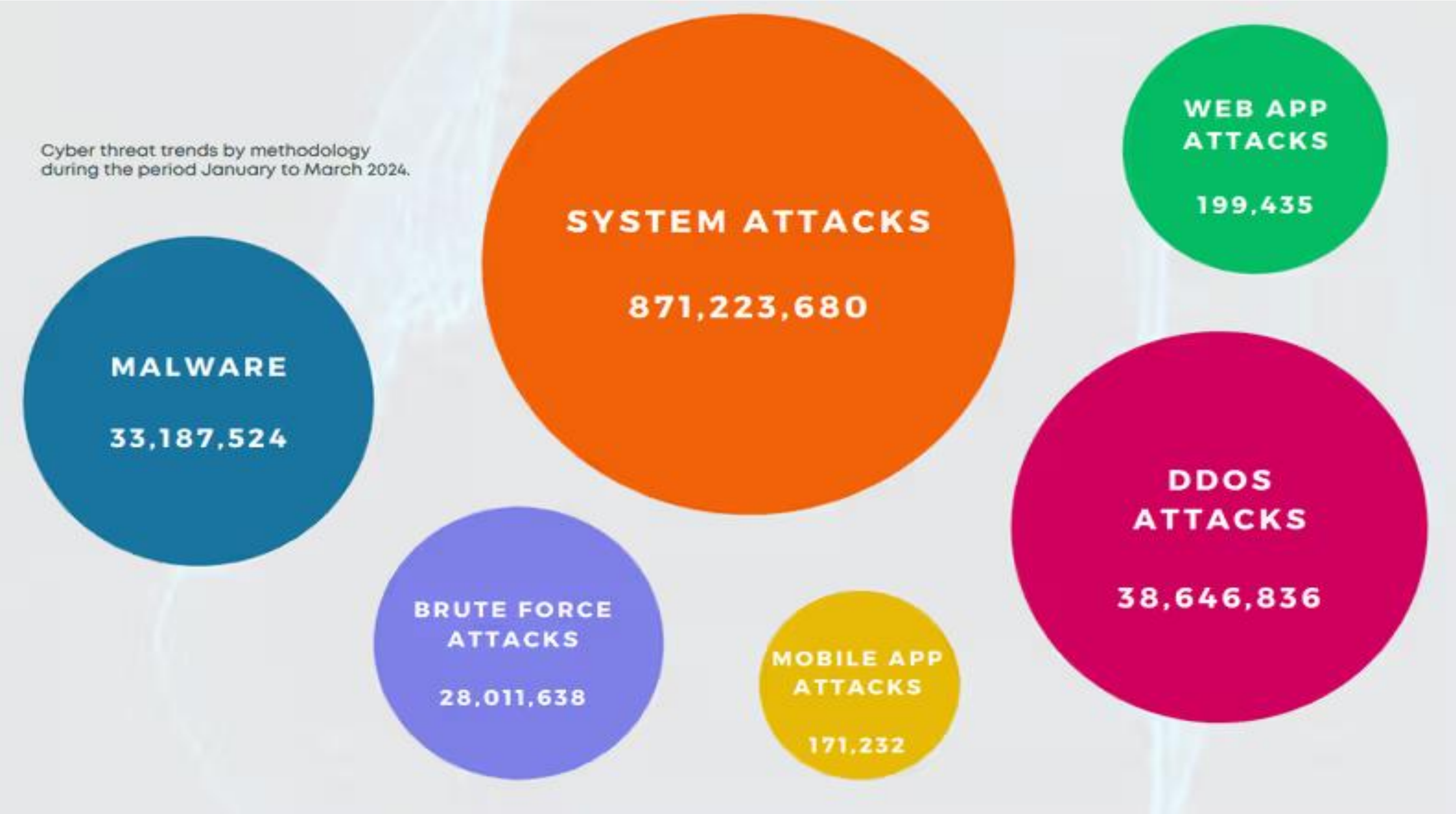
"Hackers are using ***trusted emails*** to send us "***attachment traps***". It is very difficult to safeguard against this at my firm."

"No one thinks they are going to
be **a victim of a Cyber Attack** Until it happens to **THEM**"

Types of cyber threats faced by Kenyans

Cyber Interactive

Interactive Defense, Proactive Security.



Cybersecurity Report by the Communications Authority of Kenya

Challenging Assumptions About Securing Digital Infrastructure in Pension Schemes

Pension Schemes Are Not Prime Targets for Cyberattacks.

Pension schemes hold vast amounts of sensitive financial and personal data, making them **lucrative targets for cybercriminals.**

Compliance Equals Security

Meeting **regulatory compliance standards (ISO 27001, DPA, or NIST,RBA,CBK) does not** guarantee a pension scheme is secure..

Cybersecurity is the Responsibility of the Administrator.

Cybersecurity requires a **multi-stakeholder approach** involving trustees, administrators, regulators, and even pensioners.

Third-Party Service Providers Are Secure.

Third-party risks are among the **biggest cybersecurity threats** pension schemes face today.

A Cyberattack Will Be Immediately Detected.

Many breaches go undetected for **months or even years**..

What are Pensions greatest fears?

A. Cyber Threats

B. Digital Transformation challenges

C. Fraud and Identity Theft

D. Regulatory and compliance Pressure

E. AI and automation Risks

"Are Your Pension Scheme’s Cybersecurity Measures Strong Enough to Protect Members’ Futures?“

Pension Scheme Trustees don’t need to be subject matter experts, but they *should* ***maintain a strong and current understanding*** *of* ***cybersecurity***, ***data protection***, *and the* ***impact of artificial intelligence*** **(AI).**

These areas play a growing role in **shaping the security and operational effectiveness of pension schemes**.

Why Cybersecurity Matters?

Digital protection in a vulnerable era.

In a rapidly digitizing world, cybersecurity is critical for preventing data breaches and protecting sensitive information.

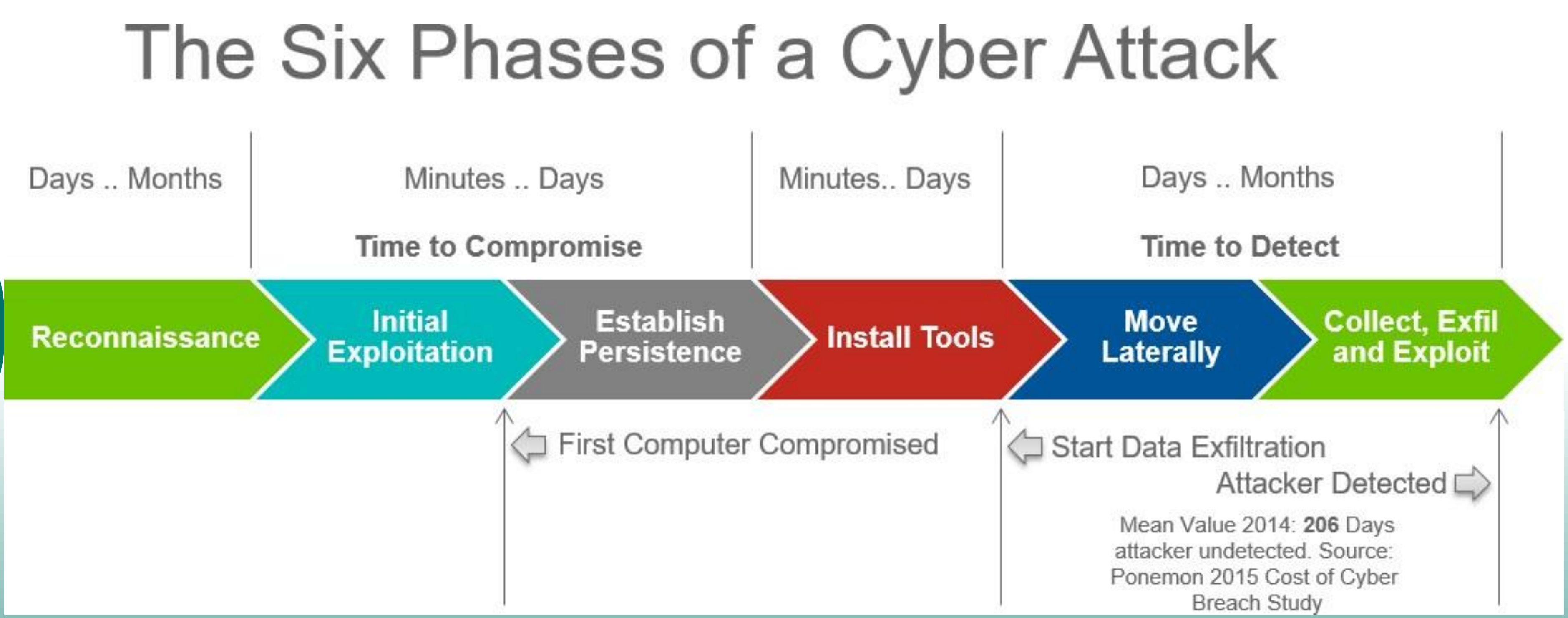
The **right strategy mitigates risks, ensuring business continuity and integrity**.

Cyber Threats Evolution

Adopting a Proactive Security Posture

Traditional security focuses largely on perimeter defenses and reactive measures. However, current trends demand a **proactive and predictive cybersecurity strategy** to anticipate threats before they occur and protect critical assets.

Phases of an Attack



The Six Phases of a Cyber Attack

Mean Value 2014: **206** Days attacker undetected. Source: Ponemon 2015 Cost of Cyber Breach Study

Key Threats in the Pension Sector

Data Breaches: Unauthorized access leading to confidential information exposure.

Phishing Attacks: Deceptive tactics aiming to trick users into revealing sensitive data.

Malware Intrusions: Covert software designed to disrupt computer systems.

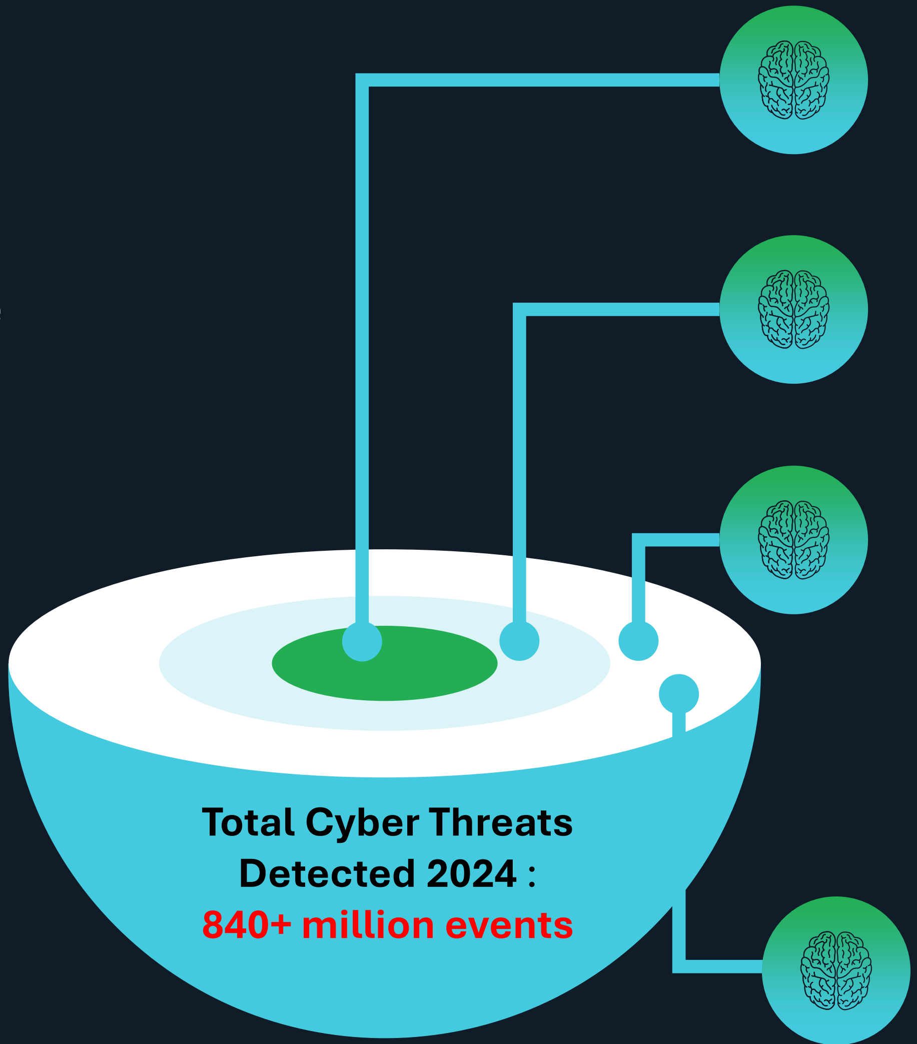
DDoS Attacks: Overwhelming a system with traffic to disrupt regular functionality.

Top 10 risks in Kenya

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 17. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2023 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	47%	*2 (29%)*	↑
2	Theft, fraud, corruption	41%	*5 (23%)*	↑
3	Changes in legislation and regulation *(e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	35%	*1 (31%)*	↓
4	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	29%	*7 (17%)*	↑
5	Business interruption *(incl. supply chain disruption)*	18%	*6 (21%)*	↑
5	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	18%	*3 (27%)*	↓
7	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	12%	*3 (27%)*	↓
7	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	12%	*7 (17%)*	→
7	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)*	12%	NEW	↑
10	Fire, explosion	6%	NEW	↑

Cybersecurity Landscape in Kenya (2024) - Most Affected Industries



Total Cyber Threats Detected 2024 :
840+ million events

Government Sector

Number of Incidents: 114 cyber-attack attempts on critical government information infrastructure (Jan - Aug 2024).

Financial Services

Number of Incidents: High-profile cases, including an attack on **Equity Bank** leading **to Ksh 179 million stolen** from 551 customers over seven days (April 2024)

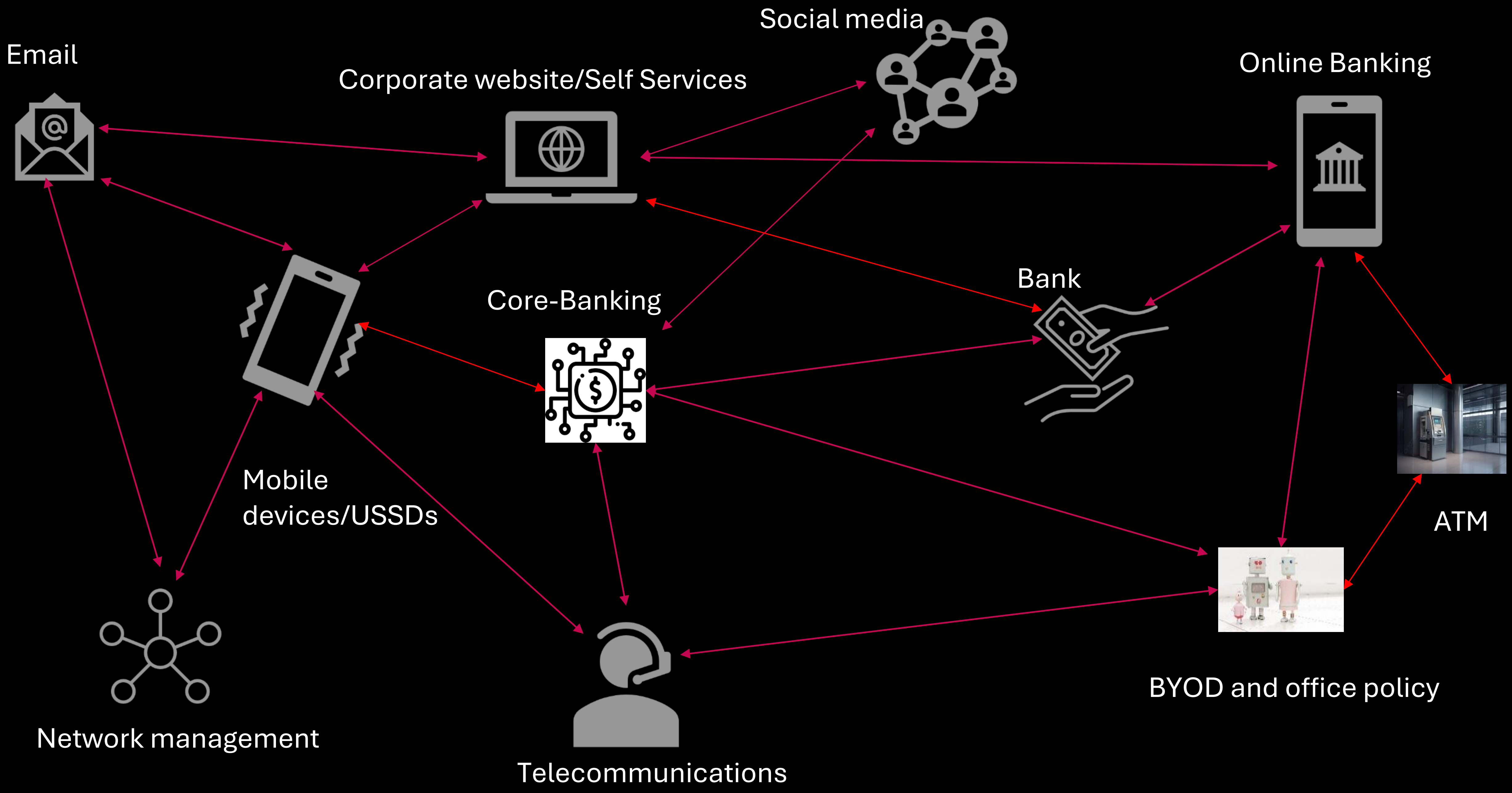
Health Sector

Number of Incidents: 15,095,217 DDoS attack attempts between October - December 2024, a **726.57% increase** from the previous quarter.

Pension Sector ?

Sources: *Communications Authority of Kenya (KE-CIRT), Nation Media, Equity Bank Reports (2024).*

Complexity of Pension Scheme Businesses



Data Breach Statistics

Cyberattacks happen once **every 39 seconds**.

95% of cyberattacks are due to **human error.**

Cybercrime cost is estimated to increase to $8 Trillion in 2024 and $10.5 Trillion in 2025

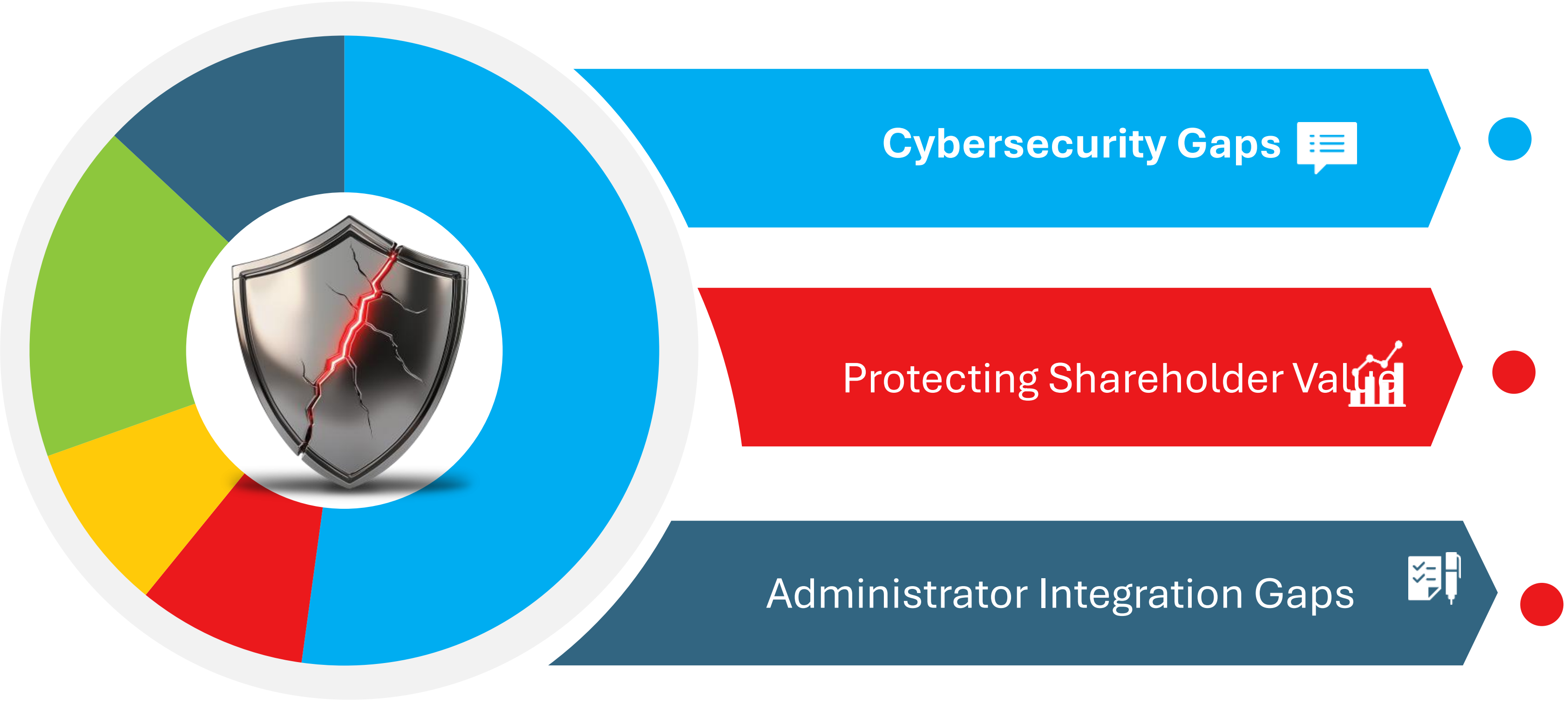
Globally, an estimated **30,000 websites** are hacked each day.

43% of Cyberattacks target **small businesses including Pensions**.

Cyber Interactive

Interactive Defense, Proactive Security.

Identified Gaps in Pension Schemes



Cybersecurity Gaps

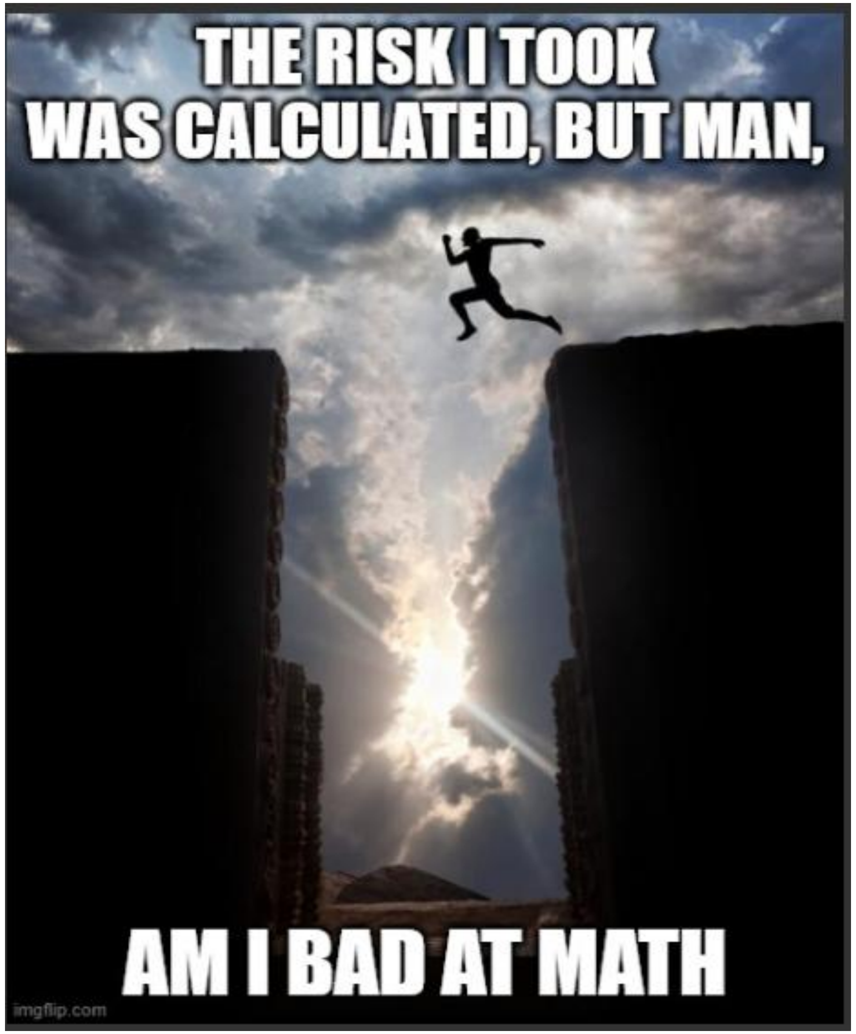
- Inadequate Cybersecurity Strategies
- Insufficient Third-Party Risk Management
- Lack of Regular Security Audits and Testing
- Inadequate Trustee and Staff Training

Protecting Shareholder Value

- Data Breaches Affecting Trust
- Limited Use of Technology to Optimize Efficiency
- Regulatory Non-Compliance Risks

Administrator Integration Gaps

- Poor Integration of Technology Across Stakeholders:
- Inconsistent Cybersecurity Protocols
- Data Sharing and Accessibility Challenges
- Lack of Real-Time Monitoring and Reporting



Key Cyber Security Risks to Pension Schemes

- Fraud and identity theft
- Social engineering and phishing
- **Ransomware attacks**
- Theft of proprietary information
- Insider threats
- **Data Breaches**
- **Third Party Exposure**
- Evolving Member expectations
- Increasing Sophistication of **Cyber Attacks**

Question ?

Which do you think is the **biggest cybersecurity threat** to pension schemes?

A. Insider fraud

B. Phishing attacks

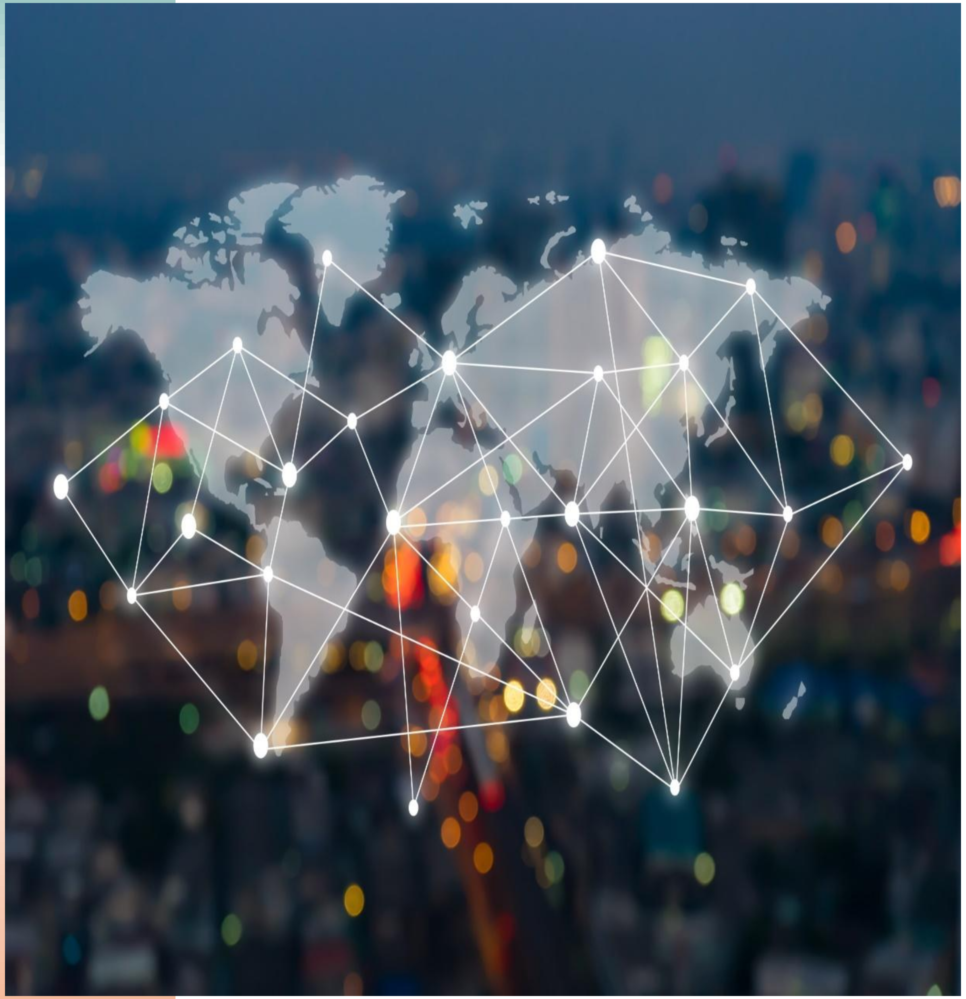
C. Weak passwords

D. Lack of compliance?

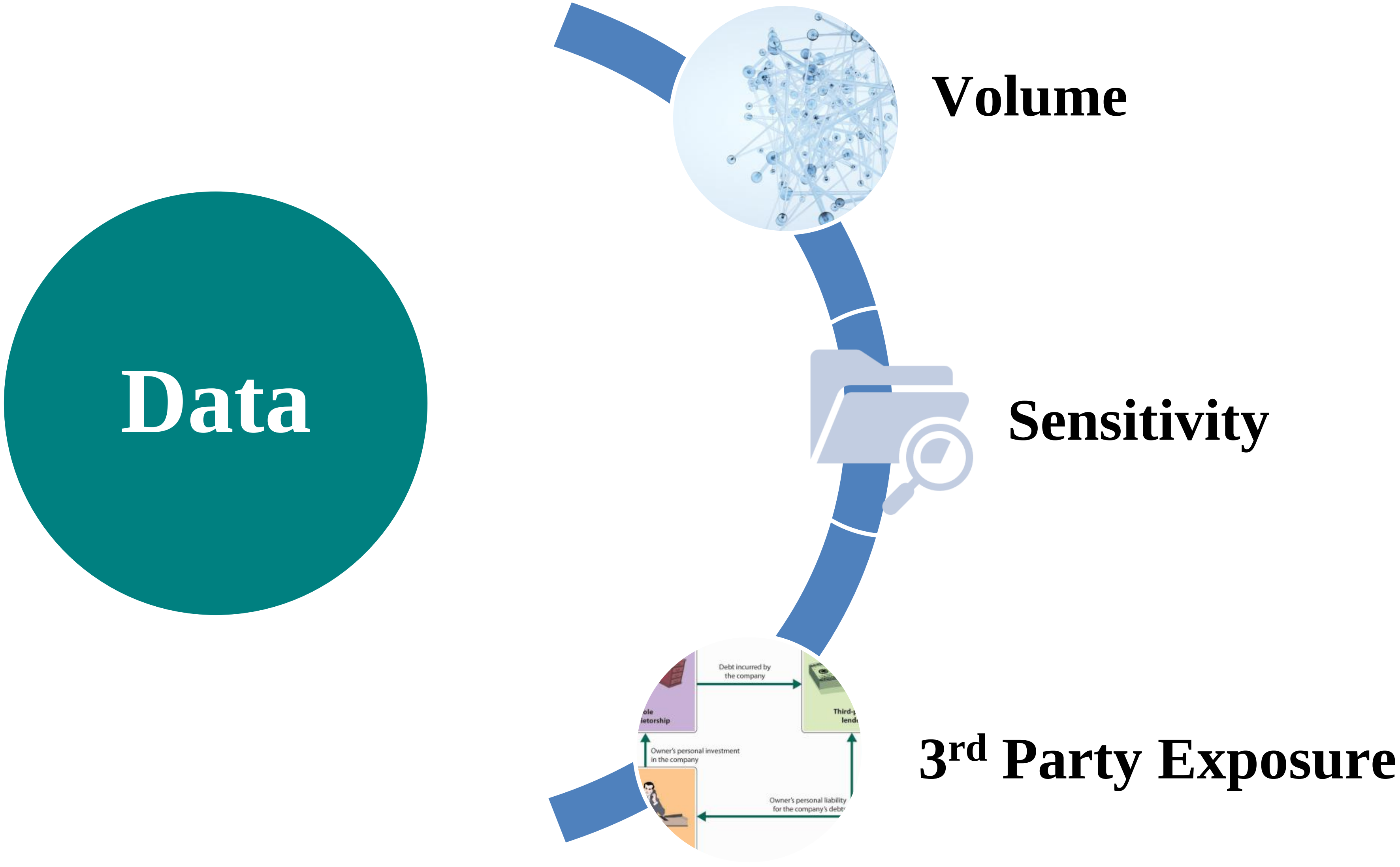
Cyber Interactive

Interactive Defense, Proactive Security.

UNDERSTANDING THE ATTACK ECOSYSTEM



Why do Cyber Criminals Target Pension Schemes



Data

Volume

Sensitivity

3rd Party Exposure

Debt incurred by the company
ole
ietorship
Third-p
lend
Owner's personal investment in the company
Owner's personal liability for the company's debt

Discussion : Five Reasons Why Pensions are not secure

We Don’t Know Ourselves
Pension administrators and organizations often lack full visibility into their IT infrastructure, cybersecurity risks, and vulnerabilities.

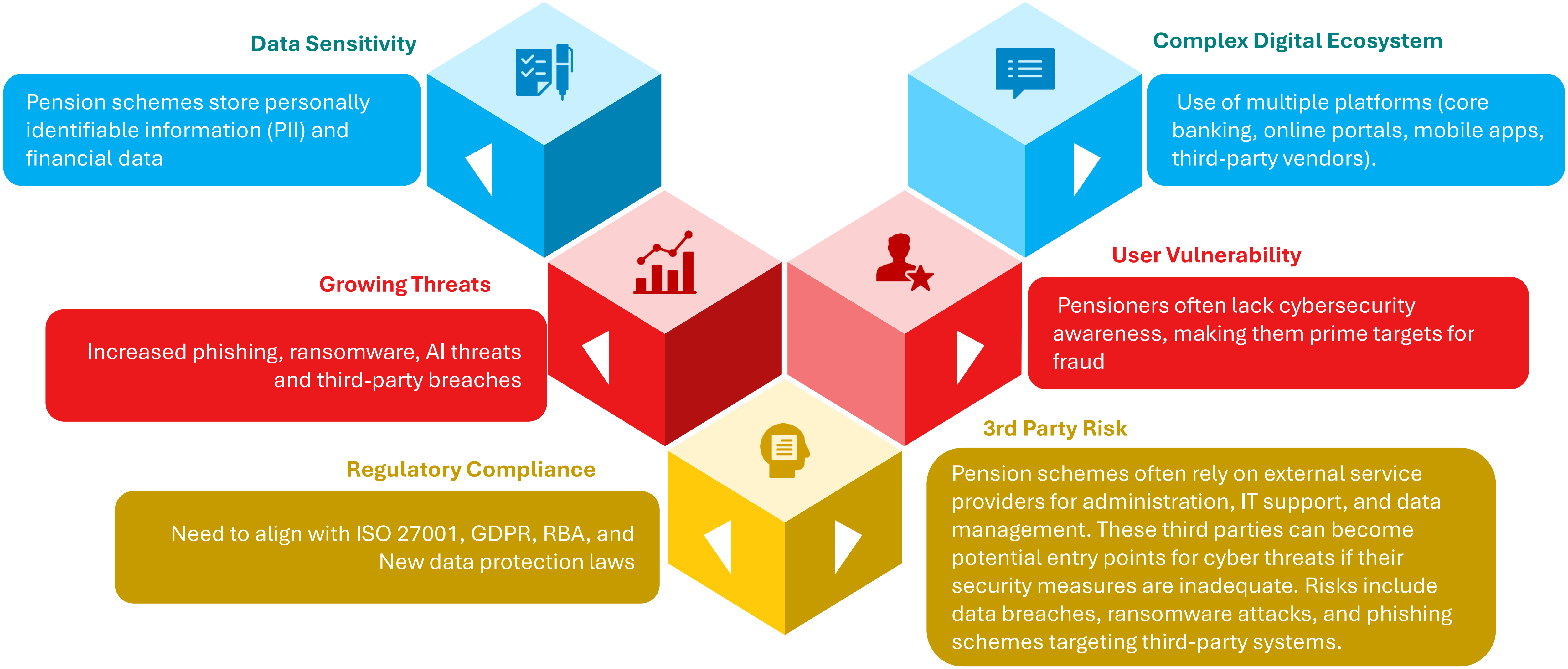
We Don’t Know Our Enemies
Many pension schemes underestimate the sophistication of modern cybercriminals, including ransomware gangs, state-sponsored hackers, and insider threats.

We Don’t Learn from (Others/Our) Mistakes
Despite past cyberattacks on pension funds globally, many organizations fail to take proactive measures.

Hackers Are Getting Smarter
Cybercriminals continuously evolve their tactics, leveraging AI-driven attacks, deepfakes, and sophisticated social engineering

Users Are More Vulnerable
Pension scheme members, especially retirees, are often prime targets for cyber fraud due to lack of awareness.

Understanding Cyber Risk in Pension Schemes



Data Sensitivity

Pension schemes store personally identifiable information (PII) and financial data

Complex Digital Ecosystem

Use of multiple platforms (core banking, online portals, mobile apps, third-party vendors).

Growing Threats

Increased phishing, ransomware, AI threats and third-party breaches

User Vulnerability

Pensioners often lack cybersecurity awareness, making them prime targets for fraud

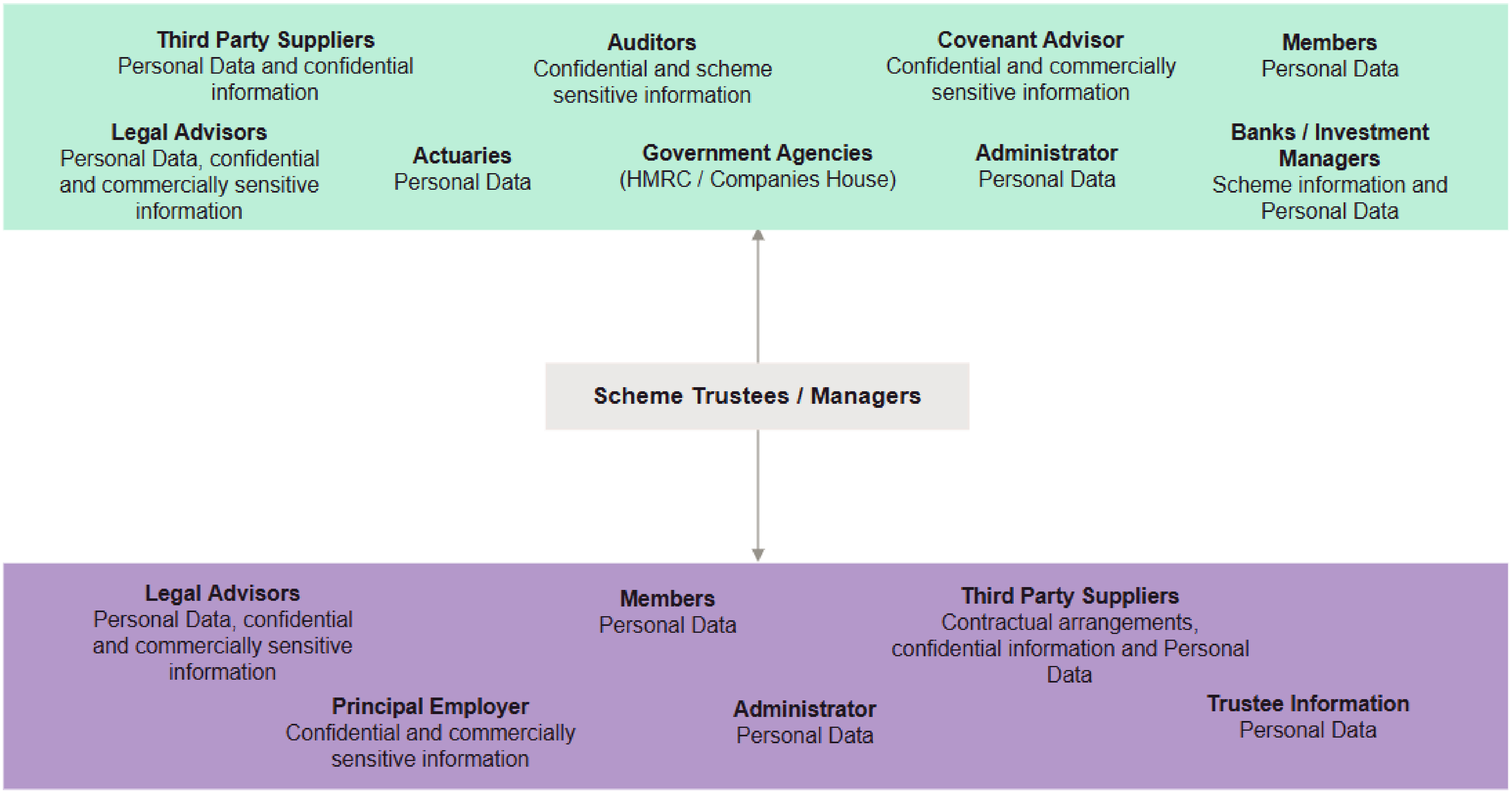
Regulatory Compliance

Need to align with ISO 27001, GDPR, RBA, and New data protection laws

3rd Party Risk

Pension schemes often rely on external service providers for administration, IT support, and data management. These third parties can become potential entry points for cyber threats if their security measures are inadequate. Risks include data breaches, ransomware attacks, and phishing schemes targeting third-party systems.

Data and Asset Map, Acritical exercise to prevent Cyber Risk



Third Party Suppliers
Personal Data and confidential information

Auditors
Confidential and scheme sensitive information

Covenant Advisor
Confidential and commercially sensitive information

Members
Personal Data

Legal Advisors
Personal Data, confidential and commercially sensitive information

Actuaries
Personal Data

Government Agencies
(HMRC / Companies House)

Administrator
Personal Data

Banks / Investment Managers
Scheme information and Personal Data

Scheme Trustees / Managers

Legal Advisors
Personal Data, confidential and commercially sensitive information

Members
Personal Data

Third Party Suppliers
Contractual arrangements, confidential information and Personal Data

Principal Employer
Confidential and commercially sensitive information

Administrator
Personal Data

Trustee Information
Personal Data

Areas of Organizational Focus

- **Insider Threats**
- External Threats
- Email Security (Business Email Compromise)
- Antimalware **vs** EndPoint Detections- Response
- Secure VPN & Control
- Active Monitoring & Incidence Response
- Actualizing Timely Mitigation Controls
- Incremental Cloud Data Backup
- Business Continuity and Strategy Alignment

Case study – Capita breach

Cyber incident overview – On **31 March 2023**, Capita plc, one of the UK's biggest pension scheme administrators, was hit by a ransomware attack by Black Basta. Black Basta posted Capita on its extortion portal on the dark web, offering to sell stolen data to interested buyers unless it paid a ransom. Examples of alleged details obtained during the cyber-attack included personal bank account details, physical addresses, passport scans, and other sensitive information.

Regulatory involvement – Following the Capita breach, The Pensions Regulator contacted 383 pension schemes which they understood to be administered by Capita. TPR also engaged with and shared information to other regulators including ICO, FCA and PRA. The ICO's investigation into the breach is ongoing.

Lessons learned – The TPR released a regulatory intervention report outlining its role in the Capita breach. This report also steps through some 'lessons learned' including in relation to communications challenges Capita experienced (time to identify exfiltrated data, communicating without contact details, agreeing template wording etc).

Financial impact – Capita has reported that the incident will cause approximately £25m in actual costs (excluding reputational damage/loss of business). Capita's share price has dropped more than 50% since the incident. Barings Law filed class action on behalf of 5,000 pension holders, including aggravated damages. They allege the claim is worth up to £5m.

What are The Pensions Regulator’s expectations?

Cyber Security Principles for pension schemes

- Assessing and understanding risk
- Controls in place
- Incident response
- Reporting

December 2023

Code of Practice

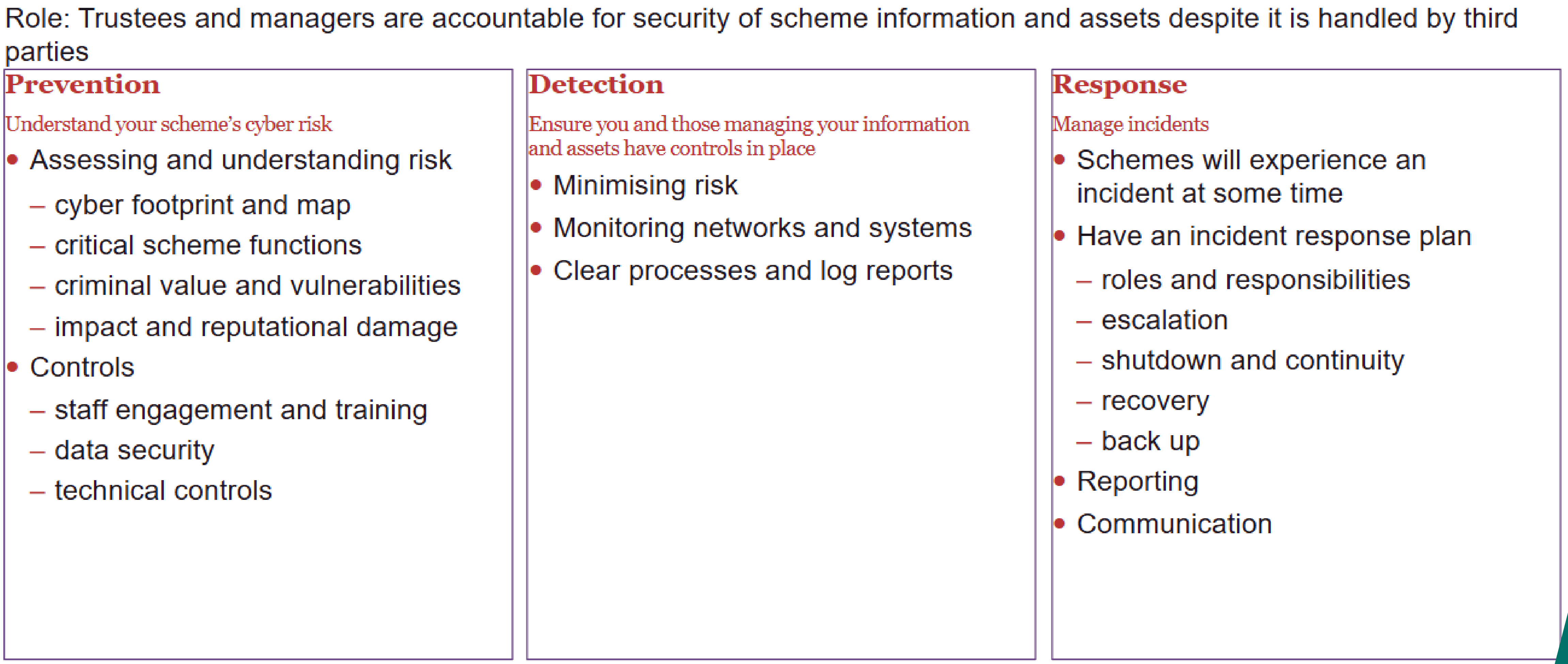
- Administration
  - IT
    - Cyber controls

March 2024

"Cybersecurity Responsibilities for Trustees & Managers: Prevention, Detection, and Response"

Cyber Interactive

Interactive Defense, Proactive Security.



Role: Trustees and managers are accountable for security of scheme information and assets despite it is handled by third parties

Prevention

Understand your scheme's cyber risk

- Assessing and understanding risk
  - cyber footprint and map
  - critical scheme functions
  - criminal value and vulnerabilities
  - impact and reputational damage
- Controls
  - staff engagement and training
  - data security
  - technical controls

Detection

Ensure you and those managing your information and assets have controls in place

- Minimising risk
- Monitoring networks and systems
- Clear processes and log reports

Response

Manage incidents

- Schemes will experience an incident at some time
- Have an incident response plan
  - roles and responsibilities
  - escalation
  - shutdown and continuity
  - recovery
  - back up
- Reporting
- Communication

Code of Practice: Cyber Controls for Governing Bodies

Incident Detection

Effective governance and internal controls

Incident Response

Consider integrations with:

- IT Systems
- Business continuity
- Governance
- Service Providers
- Data Protection Law

Assessing Risk

- Ensure governing bodies have knowledge and understanding.
- Understanding requitement for confidentiality, integrity and availability of systems for processing personal data.
- Risk register
- Test vulnerability of the scheme's key functions, systems assets to cyber incidents.
- Consider accessing specialist skills and experience.
- Ensure appropriate system controls are in place and up to date.

Managing Risk

- Critical systems and data backed up
- Policies
- DP policies are up to date.
- Maintain a cyber response plan.
- Understand service providers controls.
- Internal reporting.

Cyber Resilience Framework for Pension Schemes

Risk Assessment and Management

- Identify Assets
- Assess Threats
- Analyze Vulnerabilities
- Prioritize Risks
- Implement Controls
- Monitor and Review

Incident Response Planning

- Incident Response Team
- Incident Response Plan
- Testing and Training
- Communication Plan

Business Continuity and Disaster Recovery

- Business Impact Analysis
- Disaster Recovery Plan (DRP)
- Backup and Recovery Procedures
- Business Continuity Plan (BCP)

Third-Party Risk Management

- Vendor Risk Assessment
- Contractual Obligations
- Regular Monitoring:

Key steps trustees should take if a Cyber Security Incident Occurs

Cyber Interactive

Interactive Defense, Proactive Security.

Engage with Employers, Administrators, and Service Providers

Notify the Retirement Benefits Authority (RBA)

Report Data Breaches to the Office of the Data Protection Commissioner (ODPC)

Restore Essential Services

Protect Members’ Benefits

Communicate with Scheme Members

Monitor Suspicious Activities and Transfer Requests

Seek Assistance from the National KE-CIRT/CC

Step Process To Assess Pension Scheme Cyber Risk Level

Board awareness Sessions

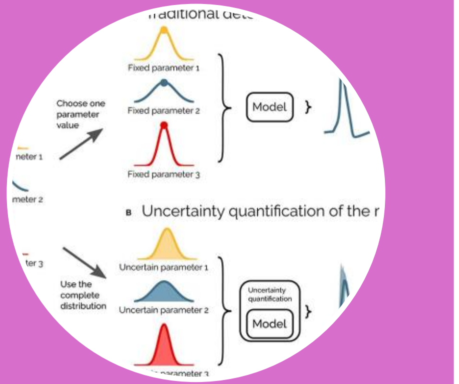
- Board awareness sessions aim to help **create a culture of better detection and readiness** within the organization should a cyber attack occur. In addition, by conducting a series of exercises and discussions, the board **gains a deeper awareness of the cybersecurity needs of its organization.**

Cyber Risk management

- Pension Schemes need to be aware of their ability to effectively manage the cybersecurity risks that they face.
- These plans should **evaluate their cybersecurity risk management programs' effectiveness and efficiency.** They will need to **define their Cyber Risk Appetite and Tolerance (RA/RT), create their Cyber Risk Management Program (CRMP) and build their Cyber Risk Target Operating Model (TOM).**

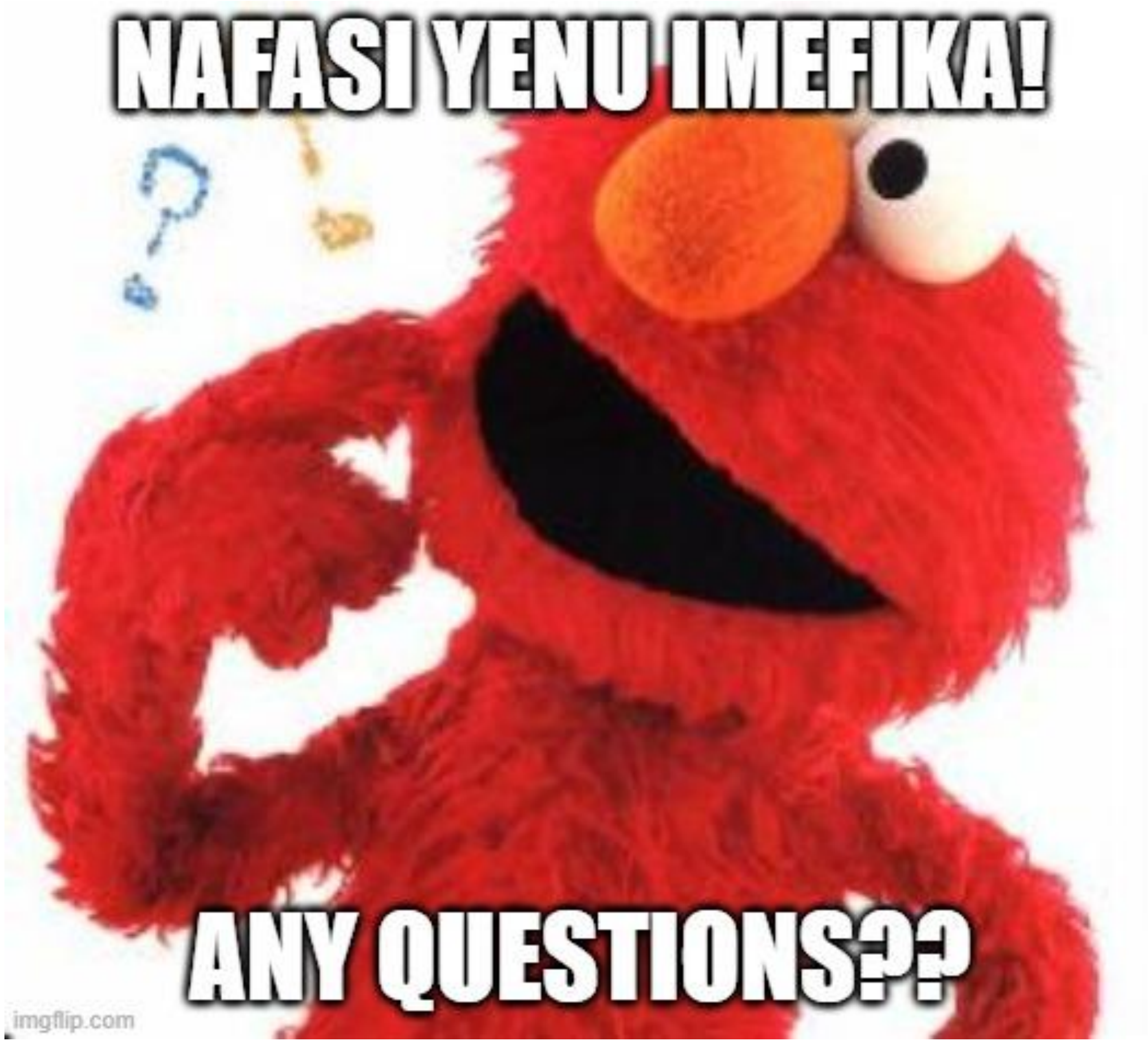
Cyber Maturity and Benchmarking

- Cyber threats multiply and become increasingly sophisticated, Pension Scheme need to understand how **mature their defenses are against them and how their cybersecurity posture** compares to that of other organizations and what Regulator expect.


Traditional de
Fixed parameter 1
Fixed parameter 2
Fixed parameter 3
Choose one parameter value
Model
B Uncertainty quantification of the r
Uncertain parameter 1
Uncertain parameter 2
Use the complete distribution
Uncertainty quantification
Model

Cyber Risk Quantification

- A Cyber Risk Quantification Approach, **where identified top risks are re-evaluated, the cyber roadmap is constructed, the cyber risk taxonomy across all lines of defense** is standardized and **specialized pieces of training on the cyber risk quantification methodologies** are conducted, is highly recommended.


NAFASI YENU IMEFIKA!
ANY QUESTIONS??
imgflip.com

Cyber Interactive

Interactive Defense, Proactive Security.

Thank you!

Kelvin Saitoti

0701 213 240 | 0782 966 418