



Transforming Cyber Risk Management



SERIANU



CVEQ™

Objectives



- Introduction
- Industry Trends and Insights
- Threat-Focused Cyber Risk Program
- Risk-Focused Cyber Risk Program
- Implementing the Risk-Focused Cyber Risk Program
- Conclusion

Vision: A world class Professional Accountancy Institute.



INTRODUCTION

Vision: A world class Professional Accountancy Institute.

About Serianu



Serianu is a Pan Africa based Cyber Security and business consulting firm. We are an award winning company in the African Cybersecurity sector that helps our customers collect, protect, and analyze critical business information.

Our Partnerships

- AFROSAI-E
- Paladion Networks - Mumbai, India
- Liquid Telecom - Africa
- USIU-Africa – Research and Data Analysis Partner







Vision: A world class Professional Accountancy Institute.

24/7 Cyber Security Centre



Vision: A world class Professional Accountancy Institute.

Africa Cyber Immersion Centre



Technical Cyber Immersion trainings are delivered at the **Africa Cyber Immersion Centre (ACIC)** in Nairobi, Kenya. ACIC emulates the environments and operations of enterprises using state-of-the-art technologies.

We simulate cyber-attacks in order to test an organisation's inherent vulnerabilities, defense and response capabilities. This facility also replicates an organisation's operating environment and uses the latest range of cyber threats, including an extensive library of viruses and malware, to simulate attacks.

Vision: A world class Professional Accountancy Institute.



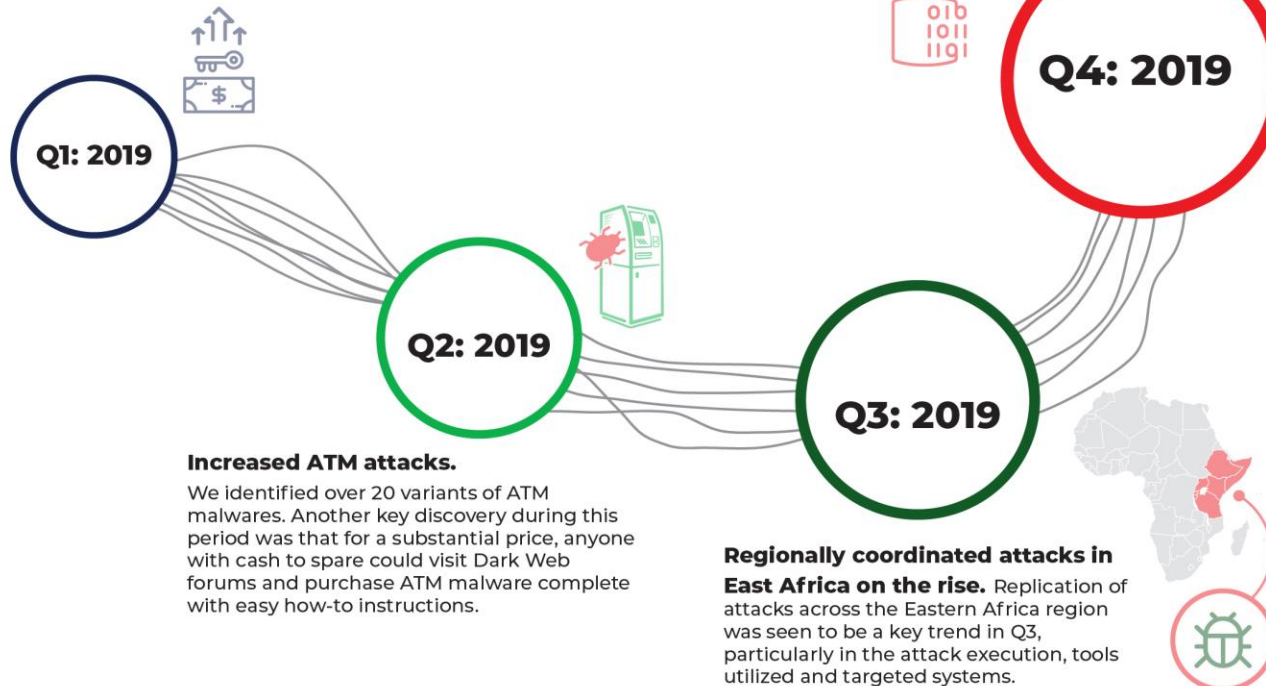
INDUSTRY TRENDS AND INSIGHTS

Vision: A world class Professional Accountancy Institute.

Key themes identified in 2019 are illustrated below:

Ransomware attacks grew by 118% globally.

On the flip side, we saw a rise in public cyber vigilance where DCI published faces and names of 130 suspected hackers in Kenya.



Q1: 2019

Q2: 2019

Q3: 2019

Q4: 2019

Increased ATM attacks.

We identified over 20 variants of ATM malwares. Another key discovery during this period was that for a substantial price, anyone with cash to spare could visit Dark Web forums and purchase ATM malware complete with easy how-to instructions.

Regionally coordinated attacks in East Africa on the rise.

Replication of attacks across the Eastern Africa region was seen to be a key trend in Q3, particularly in the attack execution, tools utilized and targeted systems.

Data protection. Kenya's first data protection law came into force. The president approved the data protection law that sets out restrictions on how personally identifiable data can be handled, stored and shared.

Key themes identified in 2020:



Q1: 2020



Unsecured remote connections grew by over 50%.

The use of remote access technologies like RDP (Remote Desktop Protocol), VPN (Virtual Private Network) skyrocketed 41% and 33%, respectively globally. Kenya registered 50% increase in unsecured connections.

Business Continuity in the face of Covid-19.

This period was a great test on the effectiveness of existing Business Continuity plans. Organisations faced both security and operational challenges as they adjusted to the travel restrictions, social-distancing regulations and sometimes loss of critical staff. On a positive note, we saw yet another display of vigilance where DCI arrested individuals suspected of hacking into NTSA and TIMS databases and issuing fake documents to Kenyans.

Q2: 2020



Q3: 2020



Gradual adoption of remote working.

As a result of the COVID-19 Pandemic, many organizations in Africa, including Kenya found themselves transitioning their business models. This involved re-architecting IT environments, processes and workforce to work from home securely.



Organized crime on the rise.

- **Kenya cyber criminals migrating to neighboring countries.**
- **Cyber criminals moving from financial services to other sectors.**
- **Social media related web scams – virtual accounts.**
- **API integration weaknesses.**
- **ATM attacks.**
- **Third Party attacks.**
- **Cloud perpetrated attacks.**
- **Crypto-mining activity on local system.**
- **Ransomware and end user system hijacking.**

Threat Scenarios



Phishing



Denial of Service



Remote Access Attacks



Third Party Attacks



Malware Distribution



Exploitation of new teleworking infrastructure



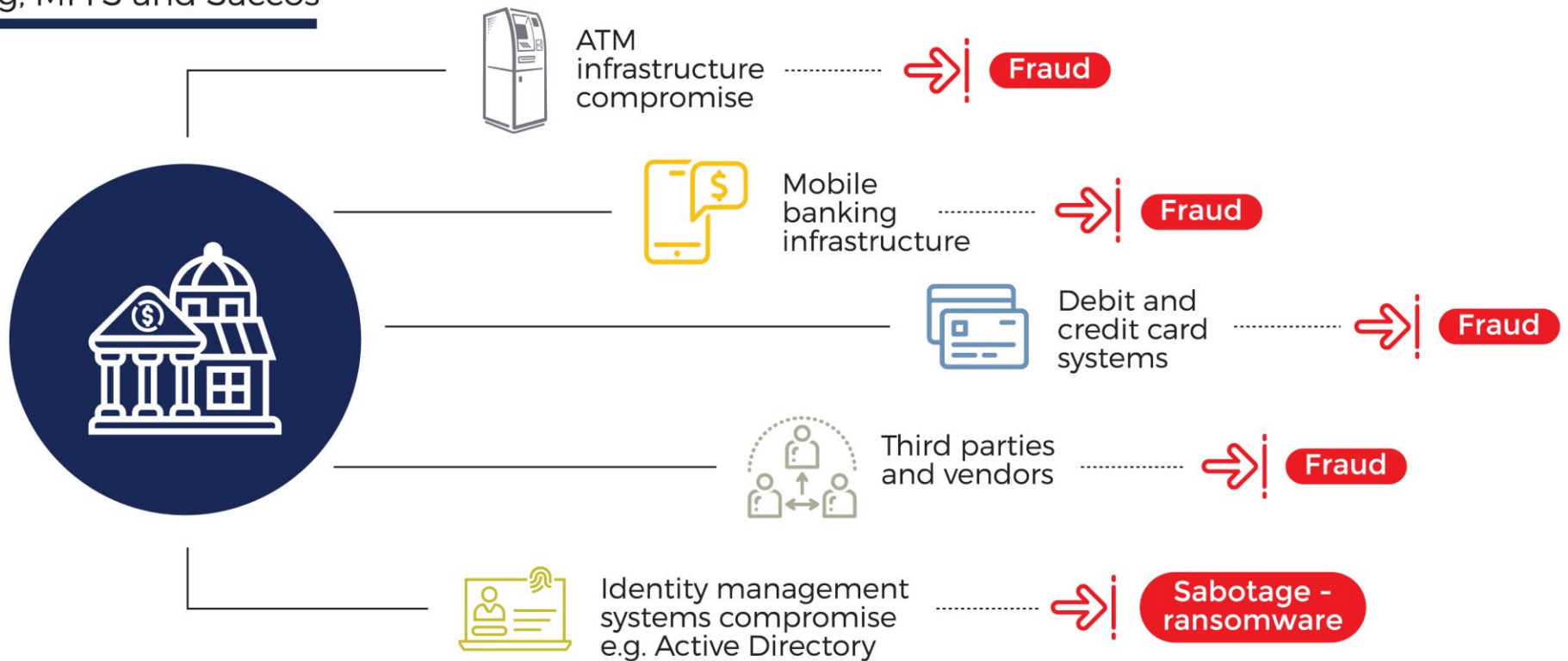
Business Email Compromise



Ransomware

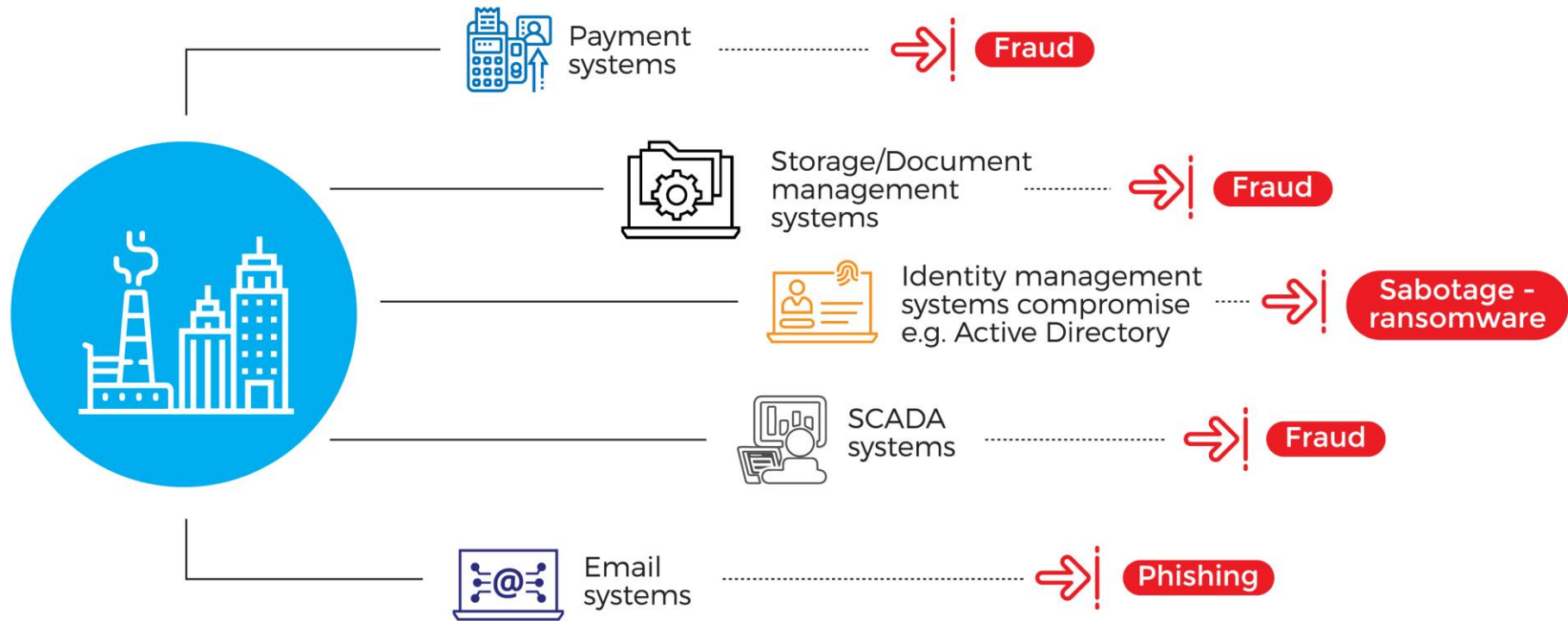
Vision: A world class Professional Accountancy Institute.

Financial Sector: Banking, MFI'S and Saccos



Others:

Manufacturing/Insurance/Healthcare/Government)



Trends



- ▶ Analytics and Automation-security operations
- ▶ Business focused metrics- risk statements (appetite, tolerance and threshold)
- ▶ Extending scope of detection and response capabilities
- ▶ Security automation and orchestration
- ▶ Privacy is becoming a major area of focus
- ▶ Embracing of cloud and Software as a Service
- ▶ Intelligence and information sharing
- ▶ Cyber Insurance and Risk Transfer (Outsourcing)
- ▶ Cyber Risk and ERM Integration

Impact



Impact	Threat Scenario	Affected Industries
Loss of Funds	<ul style="list-style-type: none">• Business Email Compromise• Payment Fraud	<ul style="list-style-type: none">• Banking• Retail and Hospitality• Legal firms• Insurance• Manufacturing
Loss of Service	<ul style="list-style-type: none">• Ransomware• Denial of Service• Employee/ Third Party Errors	<ul style="list-style-type: none">• Service providers• Health care• Finance support services• Academia
Loss of Data	<ul style="list-style-type: none">• Phishing• Data Leakage• Vulnerability Exploitation• Loss of Devices	<ul style="list-style-type: none">• Consulting and service firms• Financial services• Internet service providers• All sectors

Vision: A world class Professional Accountancy Institute.

Challenges Facing African Organisations



- Limited and **insufficient resources** (budgets)
- Lack of **adequate oversight** from **senior management** and **board**
- Lack of **affordable solutions** and **technologies**
- Use of **outdated, unsupported** and **pirated technologies**
- Lack of cyber security **awareness and education**
- Lack of **trained and experienced** cyber security professionals
- **Poorly drafted and implemented** cyber security policies, **laws and regulations**
- Lack of **locally researched and validated** cyber threat attack trends and patterns
- Low **adoption of standardized** cyber risk **management practices**
- Lack of **risk monitoring** and **threat detection capabilities**
- Low **adoption of cyber risk metrics and measurement**
- Lack of timely **access to trusted**, relevant and **actionable cyber threat intelligence**

Vision: A world class Professional Accountancy Institute.



THREAT-EXPOSURE-FOCUSED CYBER RISK PROGRAM

Vision: A world class Professional Accountancy Institute.

Traditional Cyber Risk Management Approach



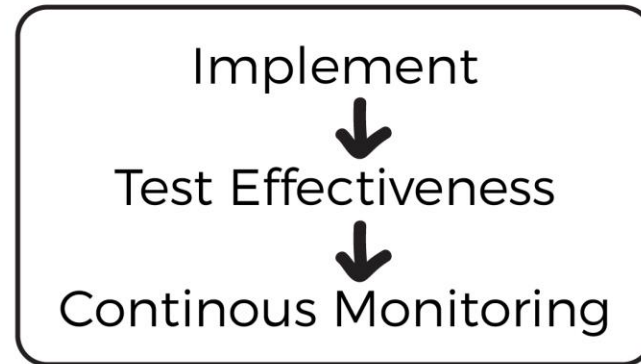
THREAT-BASED CYBER RISK MANAGEMENT PROGRAM

Risks



Register

Controls



Audit Report

Threat-Exposure-Oriented Program (SOC-Based)

Traditional Cyber Risk Management Approach



THREAT-BASED CYBER RISK MONITORING APPROACH

Threats

Threat Scenarios
Malware, Unauthorized Access, Rogue Devices, Botnet,
In-Scope Assets
Malware, Unauthorized Access, Rogue Devices, Botnet,
Monitoring Rules
User fails more than three login attempts, Specific types are copied to USB drives, Sent as email attachments to non-company domains

Incidents

Triggered Events
Malware alerts from anti-virus system, Failed logins to a critical server, Communication to a malicious IP
Detected Incidents
Malware detected on the mail server, Critical file transferred from cloud server, Firewall rule updated
Malware clean-up, File transfer incident investigated, Firewall rule changes reversed

Threat-Exposure-Oriented Program (SOC-Based)

Vision: A world class Professional Accountancy Institute.

Characteristics of Threat-Focused Approaches to Cyber Risk Management



- Reactive – based on identified incidents
- Too Technical – lack of business risk perspective
- Siloed- focuses on technology vulnerabilities
- Irregular risk audits – lack of integration to risk profiling process
- Manual and tedious – the mitigation strategy is tedious and not efficient

Challenges with the Threat-Focused Approach to Cyber Risk Management



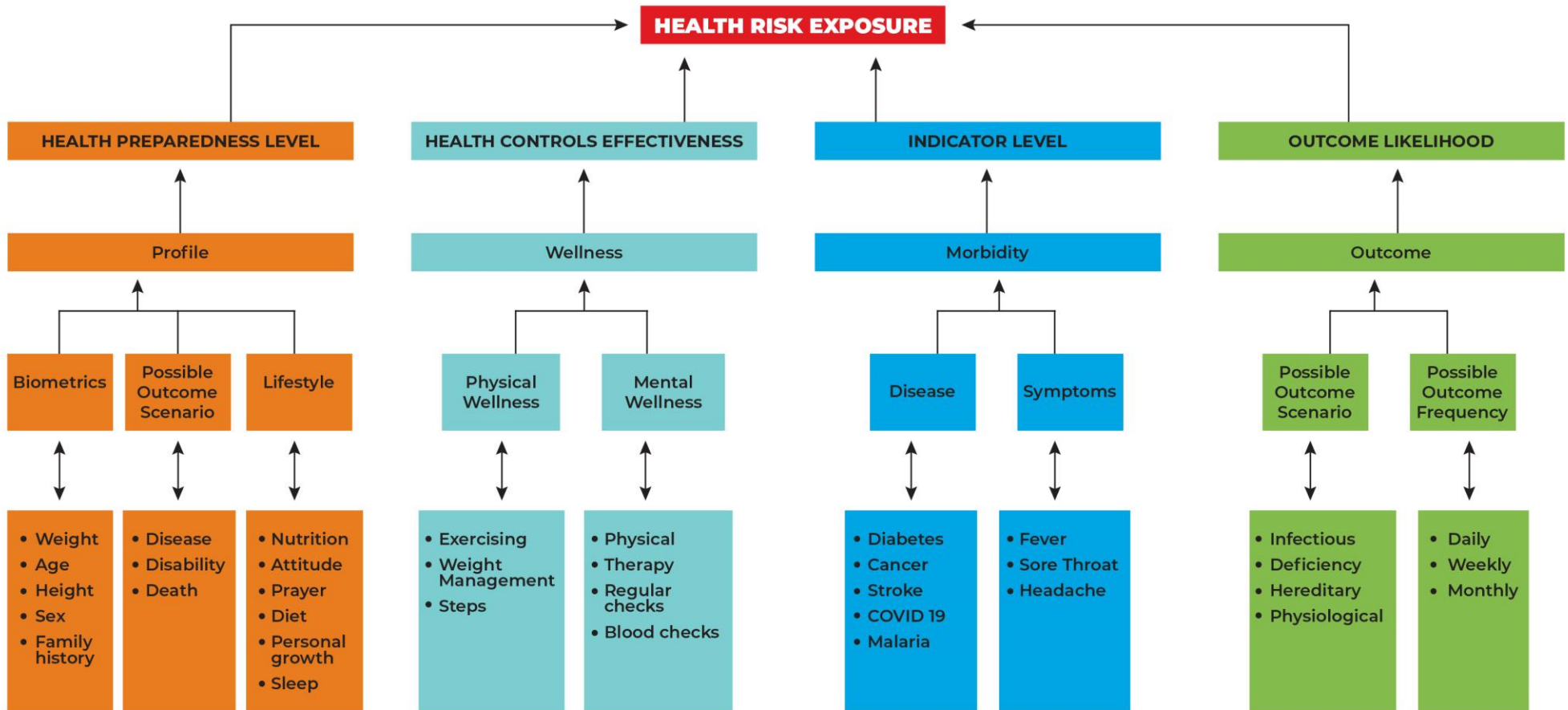
- Lack of standardized measures
- Lack of Asset information
- Informal Analysis Methods
- Focus on system level vs business level - credit risk, market risk,
Cyber risk??
- Increasing system and Ecosystem Complexity - Cloud and 3rd parties

Vision: A world class Professional Accountancy Institute.



RISK-EXPOSURE-FOCUSED CYBER RISK PROGRAM

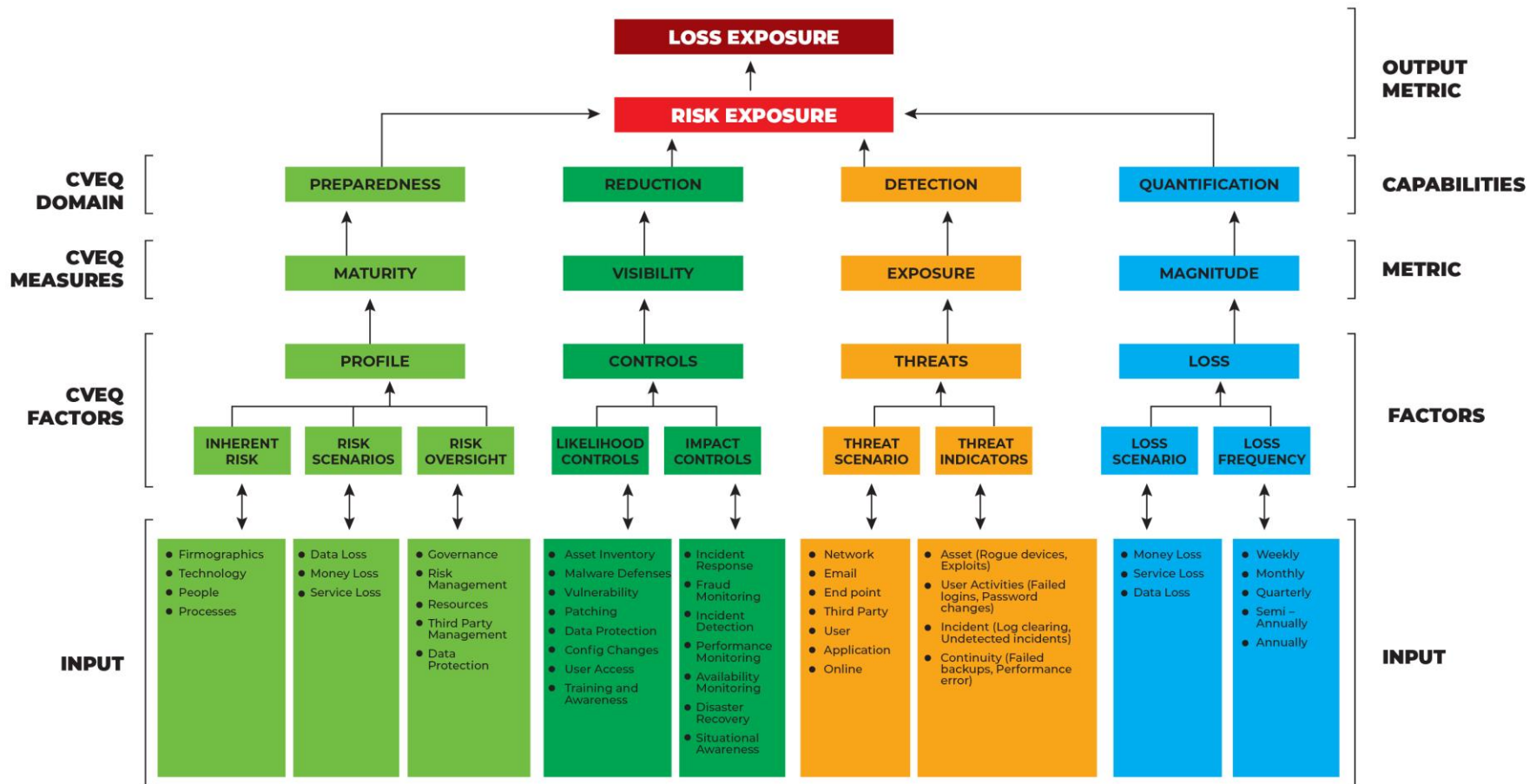
Vision: A world class Professional Accountancy Institute.





RISK AREA	HEALTH RISK MANAGEMENT	CYBER RISK MANAGEMENT
RISK PREPAREDNESS	Biometric Profile <ul style="list-style-type: none"> Weight, Height, Age, Sex, Family history 	Firmographic Profile <ul style="list-style-type: none"> Industry, Revenue, Geography, Size
	Lifestyle Profile <ul style="list-style-type: none"> Nutrition, Attitude, Prayer, Diet, Personal Growth, sleep 	Risk Oversight <ul style="list-style-type: none"> Governance, Risk Management, Resources, Third Party Management, Data Protection
RISK REDUCTION	Physical Wellness <ul style="list-style-type: none"> Exercising, Weight Management, steps 	Likelihood Controls <ul style="list-style-type: none"> Malware, Vulnerabilities, Configuration changes
	Medical wellness <ul style="list-style-type: none"> Physical Therapy, Regular checks, blood checks, Dental 	Impact Controls <ul style="list-style-type: none"> Transaction monitoring, Incident response, Disaster recovery, Situation Awareness
RISK DETECTION	Disease <ul style="list-style-type: none"> Diabetes, Cancer, Stroke, COVID 19, Malaria 	Threats <ul style="list-style-type: none"> Malware, Ransomware, Rogue Device, Insider, Espionage
	Symptoms <ul style="list-style-type: none"> Fever, Sore throat, Headache 	Threat Indicators <ul style="list-style-type: none"> Failed Logon, Database modifications, performance degradation, User account deletion
RISK QUANTIFICATION	Morbidity Likelihood <ul style="list-style-type: none"> Infectious, deficiency, hereditary, physiological 	Risk Exposure <ul style="list-style-type: none"> Unauthorized data transfer, unauthorized data disclosure, unplanned resource unavailability, unauthorized funds transfer
	Mortality Likelihood <ul style="list-style-type: none"> Infectious, deficiency, hereditary, physiological 	Loss Exposure <ul style="list-style-type: none"> Fraud, Sabotage, Data Loss/ Theft

Vision: A world class Professional Accountancy Institute.



Emerging Approaches to Cyber Risk Management



Organisations need to:

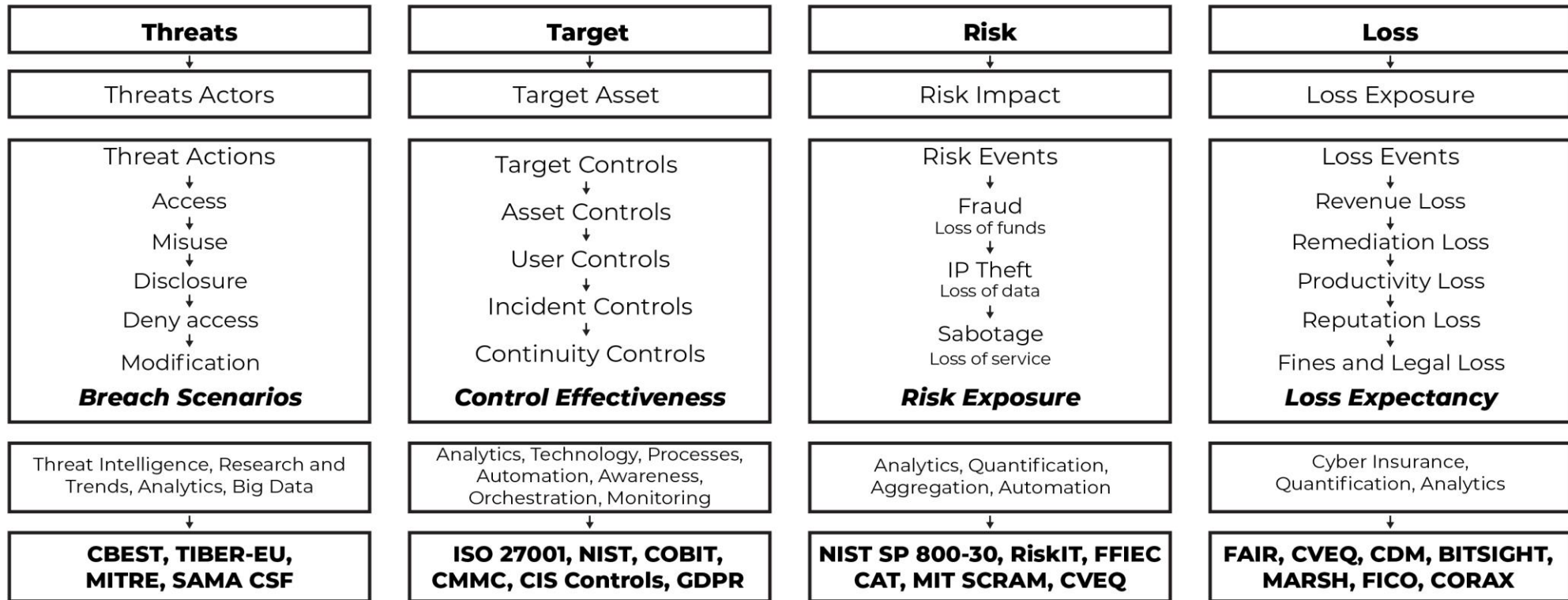
- Move Cyber risk management to the same level as other areas of risk, not just **an IT issue**
- Understand the **legal implications** of cyber risks as they relate to their **company's specific circumstances**
- Have adequate **access to cybersecurity expertise**, and discussions about cyber risk management should be given **regular and adequate time** on board meeting agendas.
- Set the **expectation and establish** an enterprise wide cyber risk management framework with **adequate staffing and budget**
- Ensure Board management discuss **cyber risk management options** including strategies to avoid, accept, **transfer or mitigate cyber risk**. This should include specific plans for each option.

Characteristics of Risk-Focused Approaches to Cyber Risk Management



- Proactive – based on the business profile
- Business focused – lack of business inherent risk
- Collaborative - expands scope to include audit, risk and operational functions
- Regular and continuous risk audits –
- Automated and efficient response – the mitigation strategy is tedious and not efficient

Risk-based Cyber Risk Management Program



RISK-EXPOSURE ORIENTED PROGRAM (ROC-BASED)

Vision: A world class Professional Accountancy Institute.

Acronyms and Definitions



- CBEST - The Council for Registered Ethical Security Testers – UK Based
- TIBER-EU - Threat Intelligence-based Ethical Red Teaming (TIBER-EU)- European Union
- MITRE ATTACK® - Cyber Offensive Tactics and Techniques – US based
- MITRE SHIELD – Cyber Defensive Tactics and Techniques – US based
- SAMA CSF – Saudi Arabian Monetary Authority Cybersecurity Framework- Saudi Arabia
- ISO 27001- international Organization For Standardization- Global
- NIST – National Institute of Standards And Technology – US based
- COBIT – Control Objectives for Information and Related Technology - Global
- CMMC – CyberSecurity Maturity Model Certification- US Government
- GDPR – General Data Protection Regulation - EU
- FAIR – Factor Analysis of Information Risk - US
- CVEQ – Cyber Visibility and Exposure Quantification – Kenya/Africa
- CDM – Continuous diagnostic and mitigation – US Military

Characteristics of a Mature Cyber Risk Program



- **Appropriate** policies and procedures are **clearly defined** and documented
- **Cost effective security** technologies are **providing their intended value**
- An **effective education and awareness** program exists
- Personnel roles and responsibilities are properly **defined and staffed**
- Board of directors are **getting the information they need**
- A risk register is used to **track and report the most important risks**
- A **clearly defined risk appetite actively** drives decision making
- Meaningful **metrics are leveraged to manage risk** effectively

Vision: A world class Professional Accountancy Institute.



CONCLUSION

Vision: A world class Professional Accountancy Institute.

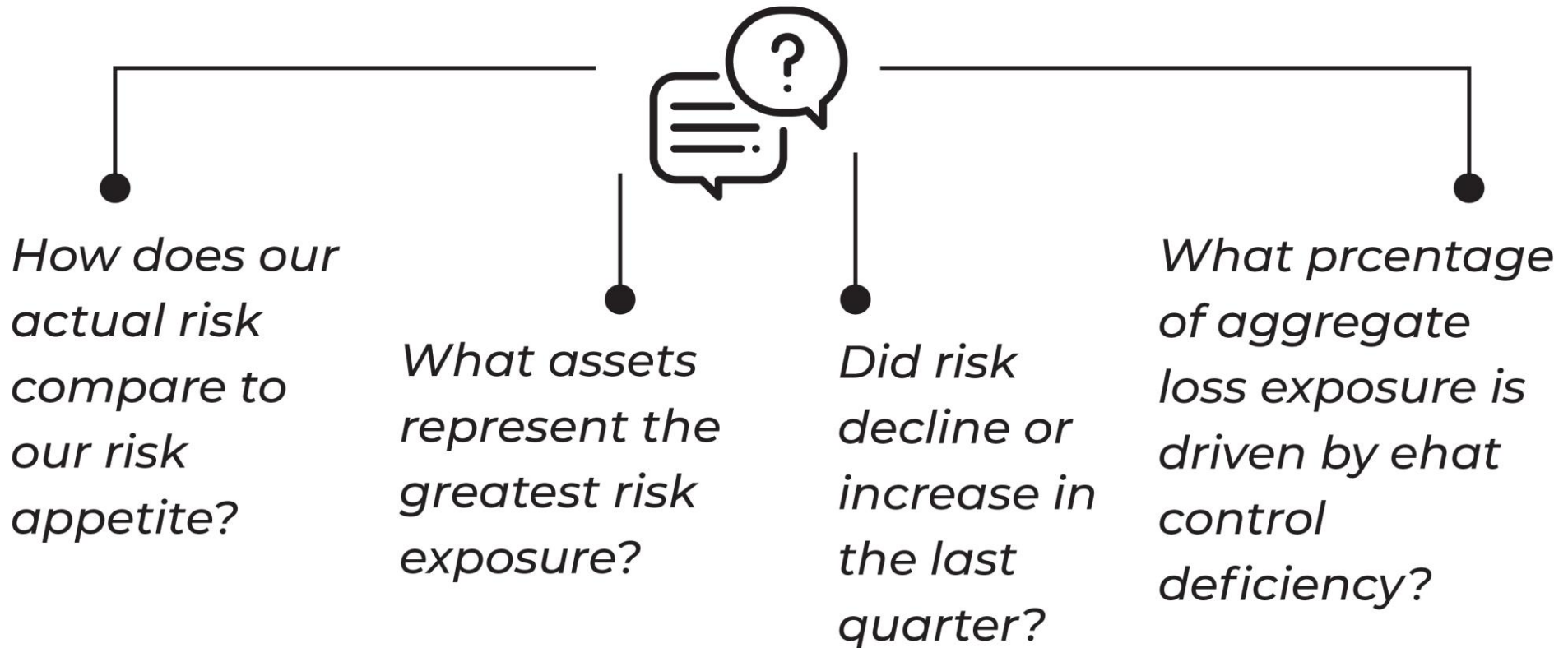
Embarking on the Cyber Security Transformation Journey



- > Create meaningful measurements to understand risks in our environment*
- > Prioritize and invest in capabilities that address risks*
- > Effectively communicate risks across the business*

Vision: A world class Professional Accountancy Institute.

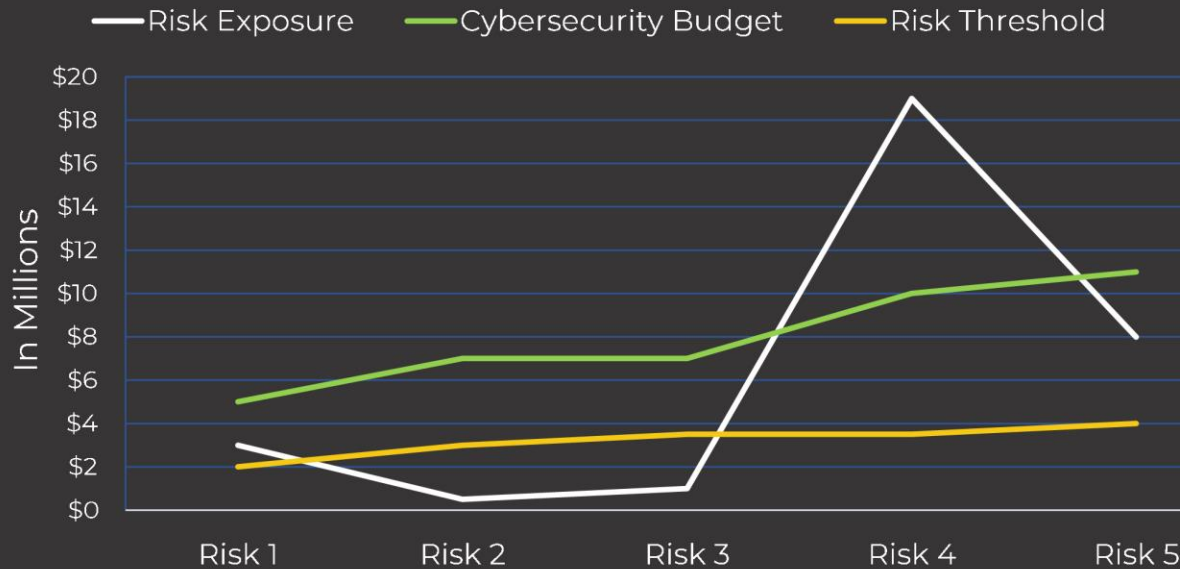
Communicating Cyber Risk in Financial Terms



Cyber Risk Quantification – Sample Report



THE TOP 5 CYBER RISKS IN FINANCIAL TERMS



Threat Scenario	Risk Exposure	Risk Probability (Annually)	Annual Frequency	Loss Exposure
Actor: Cyber criminal Motivation: Financial Gain Vector: Ransomware	Loss of data and or loss of service	40%	1 event per year	19 Million
Payment System Compromise	Loss of money	50%	2 events per year	15 Million
Phishing and Business Email Compromise	Loss of money	60%	4 events per year	20 Million
Credential Misuse	Loss of data	40%	2 events per year	8 Million
System Upgrade	Loss of availability	30%	1 event per year	1 Million
Vendor Compromise	Loss of data	30%	1 event per year	3 Million

Vision: A world class Professional Accountancy Institute.

Embedding Cyber Risk in the ERM Program



RISK DRIVERS FOR MARKET, CREDIT AND CYBER RISK

COMPONENT	MARKET RISK	CREDIT RISK	CYBER RISK
EXPOSURE	Investment Portfolio	Loan Portfolio	Digital assets portfolio; corporate brand & reputation
PROBABILITY	Probability of loss or gain <ul style="list-style-type: none"> Market price volatility 	Probability of default <ul style="list-style-type: none"> Economic conditions Credit ratings 	Probability of breach <ul style="list-style-type: none"> Threat vectors Preventative controls
SEVERITY	Holding period <ul style="list-style-type: none"> Market liquidity of investments 	Loss in the event of default <ul style="list-style-type: none"> Collateral rights Bankruptcy rights 	Loss in the event of breach <ul style="list-style-type: none"> Dwell time Resolution time Detective, mitigation and proactive controls
CORRELATION	Price correlations <ul style="list-style-type: none"> Asset allocation Position concentrations 	Default correlations <ul style="list-style-type: none"> Loan concentrations Country/ industry diversification 	Threat/ control correlations <ul style="list-style-type: none"> Cyber attack patterns Central points of failure: IT infrastructure, supply chain

Vision: A world class Professional Accountancy Institute.



Serianu Limited

14 Chalbi Drive, Lavington, Nairobi, Kenya

General Information: +254 (0) 20 200 6600

Cyber Crime Hotline: +254 (0) 800 22 1377

info@serianu.com

www.serianu.com

Vision: A world class Professional Accountancy Institute.