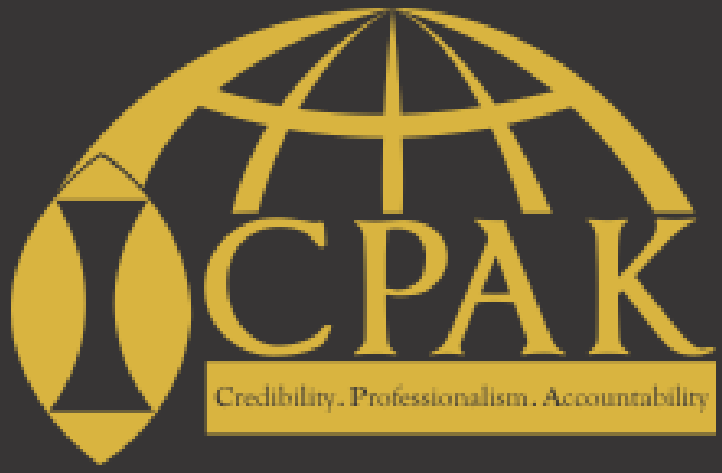


Transforming Cyber Risk Management

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

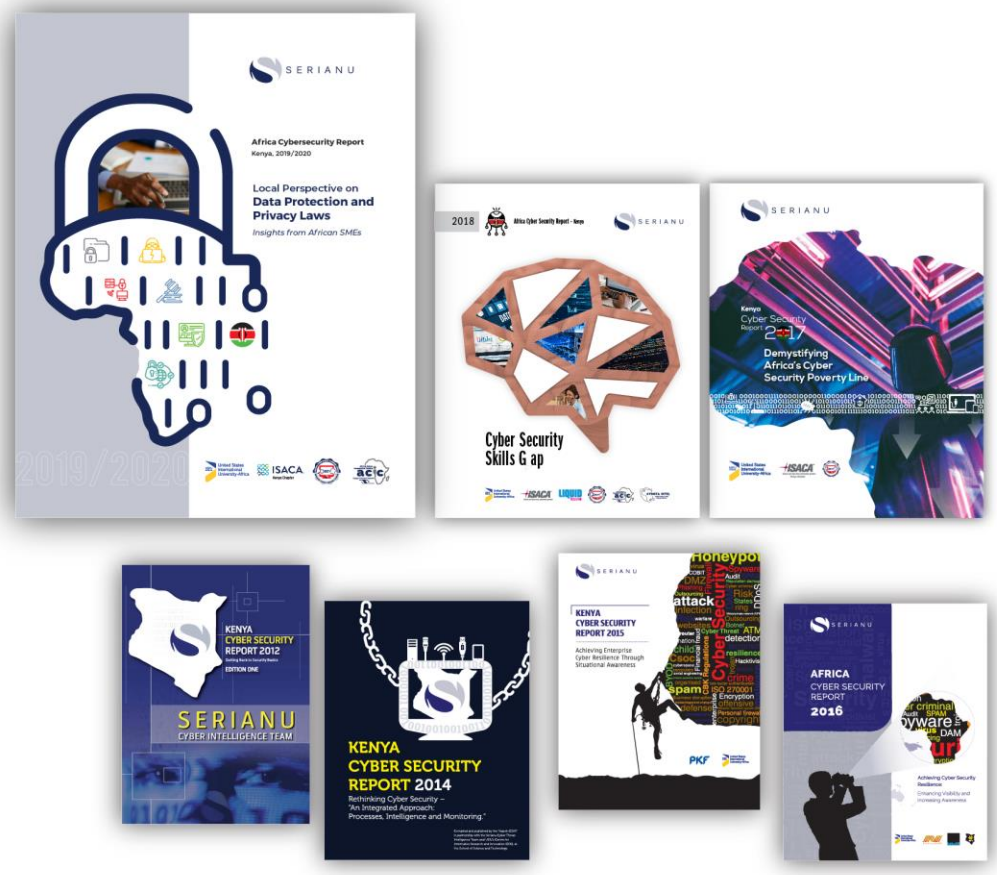
INTRODUCTION

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

ICPAK
Credibility. Professionalism. Accountability

Vision: A world class Professional Accountancy Institute.

Africa Cyber Immersion Centre

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

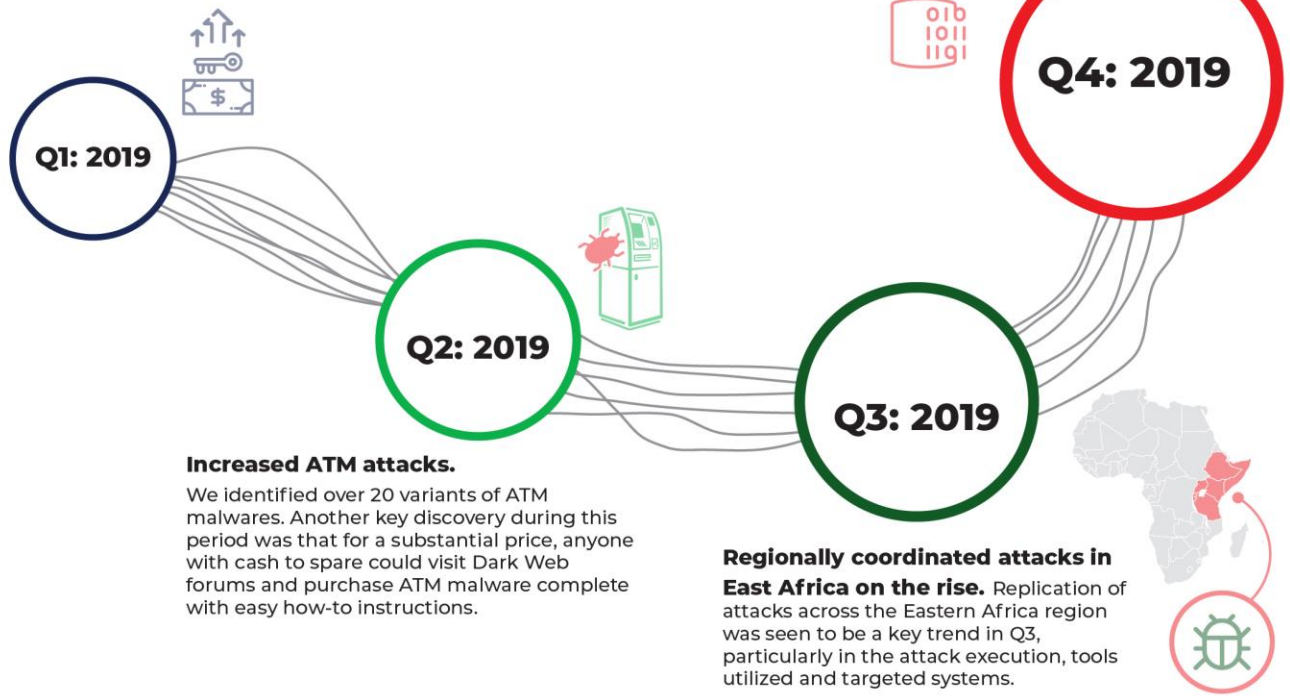
Technical Cyber Immersion trainings are delivered at the **Africa Cyber Immersion Centre (ACIC)** in Nairobi, Kenya. ACIC emulates the environments and operations of enterprises using state-of-the-art technologies.

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

Key themes identified in 2019 are illustrated below:



Q1: 2019

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.

Q2: 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.

Q3: 2019

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.

Q4: 2019

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

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

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.

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

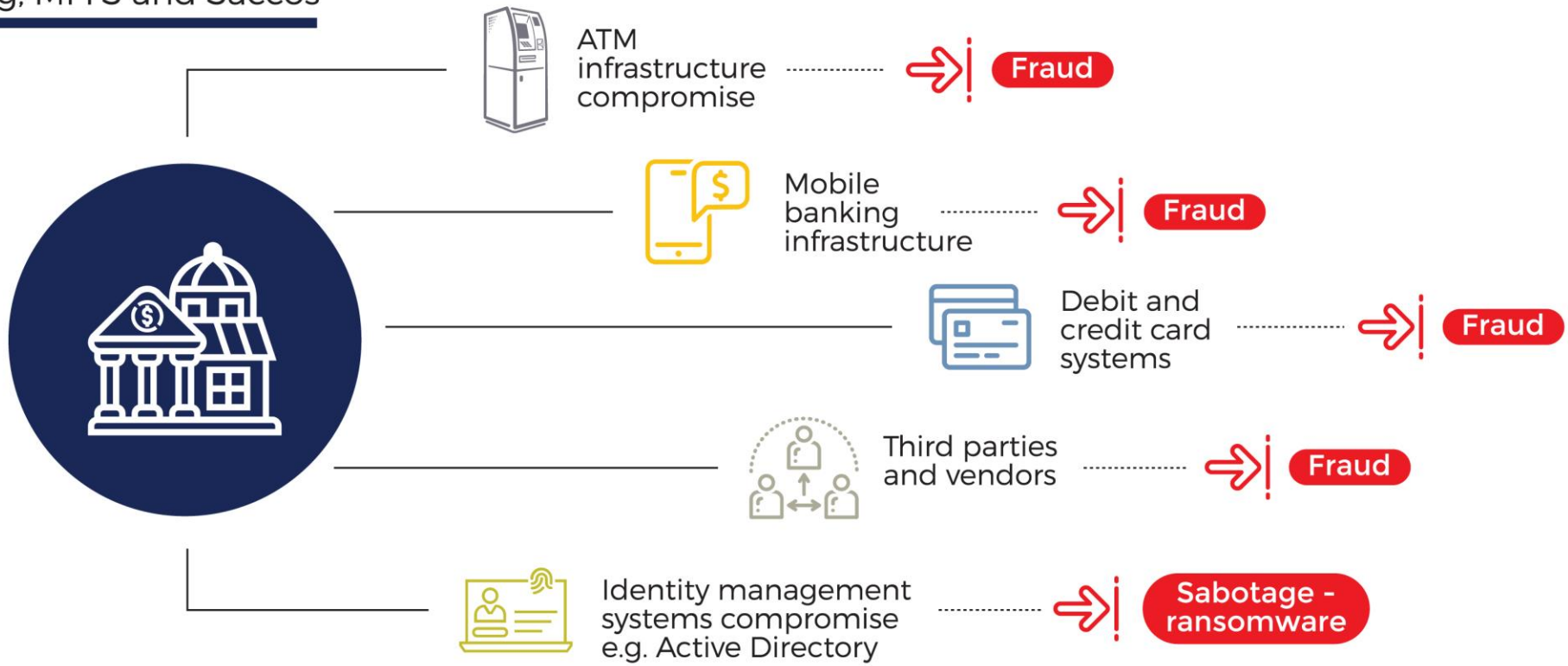
Malware Distribution

Exploitation of new teleworking infrastructure

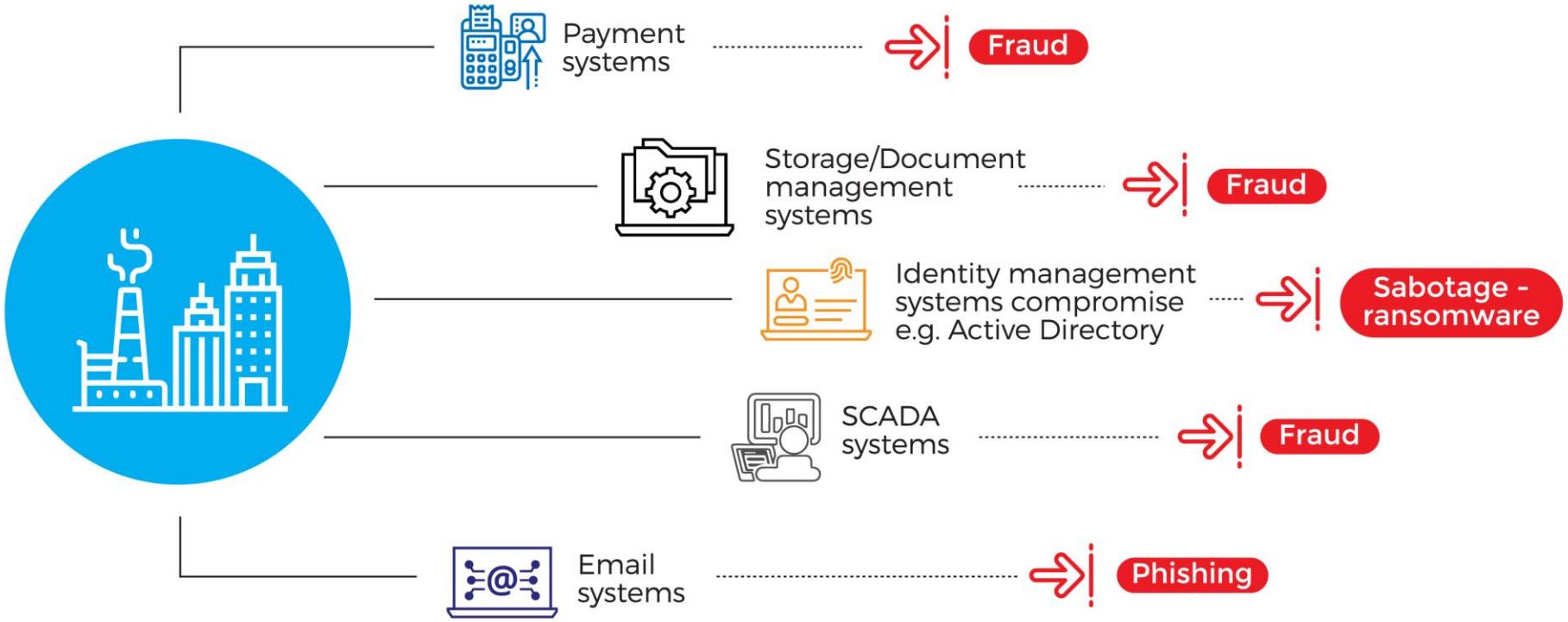
Business Email Compromise

Ransomware

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

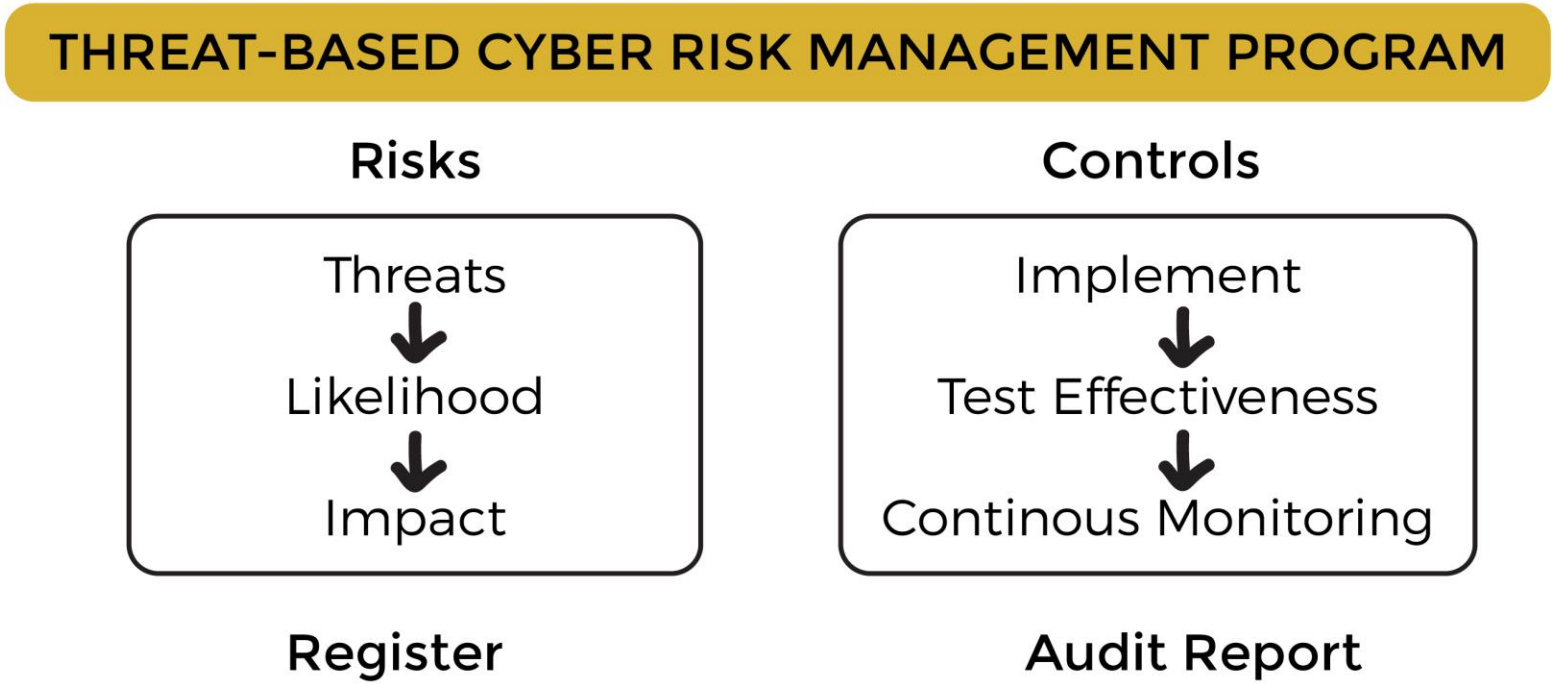
Impact	Threat Scenario	Affected Industries
Loss of Funds	• Business Email Compromise • Payment Fraud	• Banking • Retail and Hospitality • Legal firms • Insurance • Manufacturing
Loss of Service	• Ransomware • Denial of Service • Employee/ Third Party Errors	• Service providers • Health care • Finance support services • Academia
Loss of Data	• Phishing • Data Leakage • Vulnerability Exploitation • Loss of Devices	• Consulting and service firms • Financial services • Internet service providers • All sectors

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**

THREAT-EXPOSURE-FOCUSED CYBER RISK PROGRAM

Traditional Cyber Risk Management Approach



Traditional Cyber Risk Management Approach

THREAT-BASED CYBER RISK MONITORING APPROACH

Threats	Incidents
Threat Scenarios	**Triggered Events**
Malware, Unauthorized Access, Rogue Devices, Botnet,	Malware alerts from anti-virus system, Failed logins to a critical server, Communication to a malicious IP
In-Scope Assets	**Detected Incidents**
Malware, Unauthorized Access, Rogue Devices, Botnet,	Malware detected on the mail server, Critical file transferred from cloud server, Firewall rule updated
Monitoring Rules	
User fails more than three login attempts, Specific types are copied to USB drives, Sent as email attachments to non-company domains	Malware clean-up, File transfer incident investigated, Firewall rule changes reversed

Threat-Exposure-Oriented Program (SOC-Based)

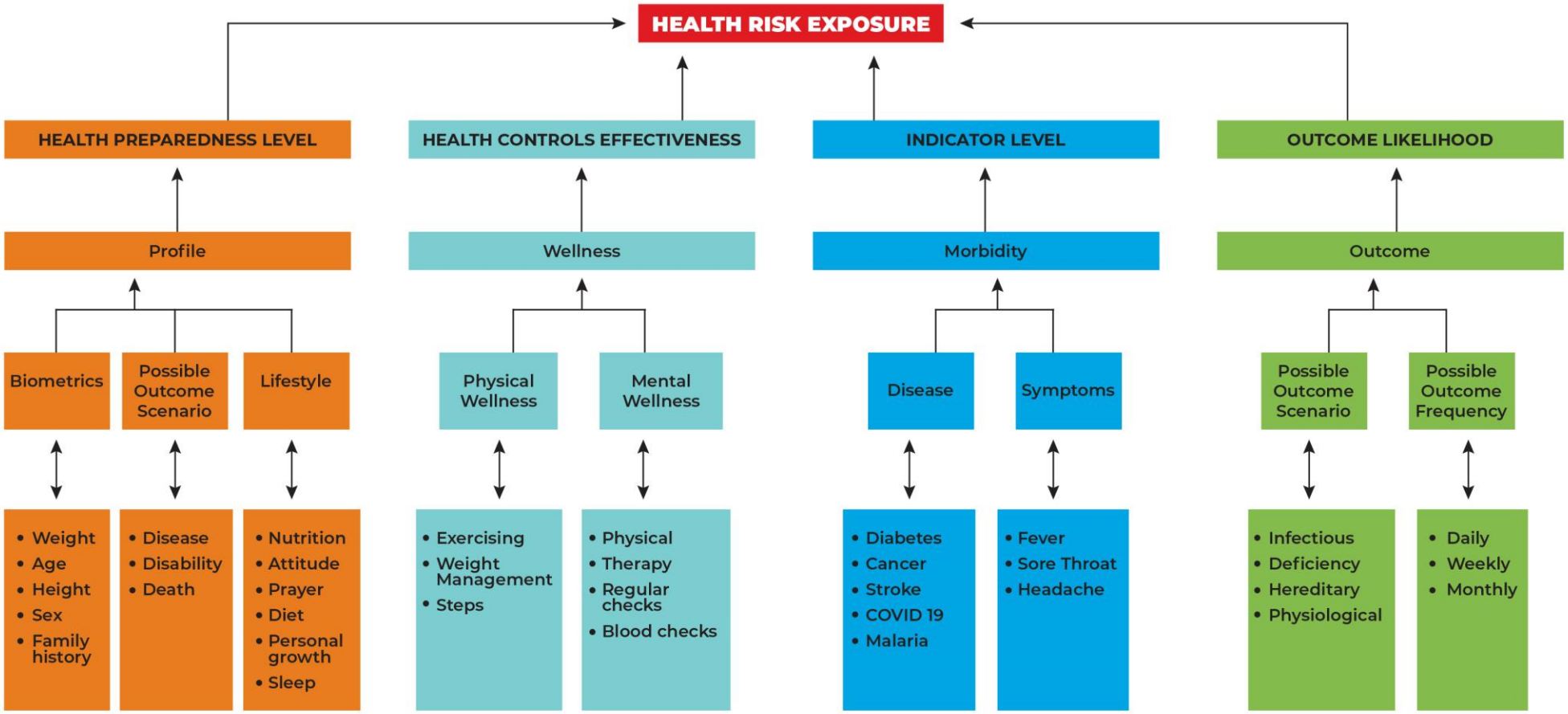
Characteristics of Threat-Focused Approaches to Cyber Risk Management

- 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

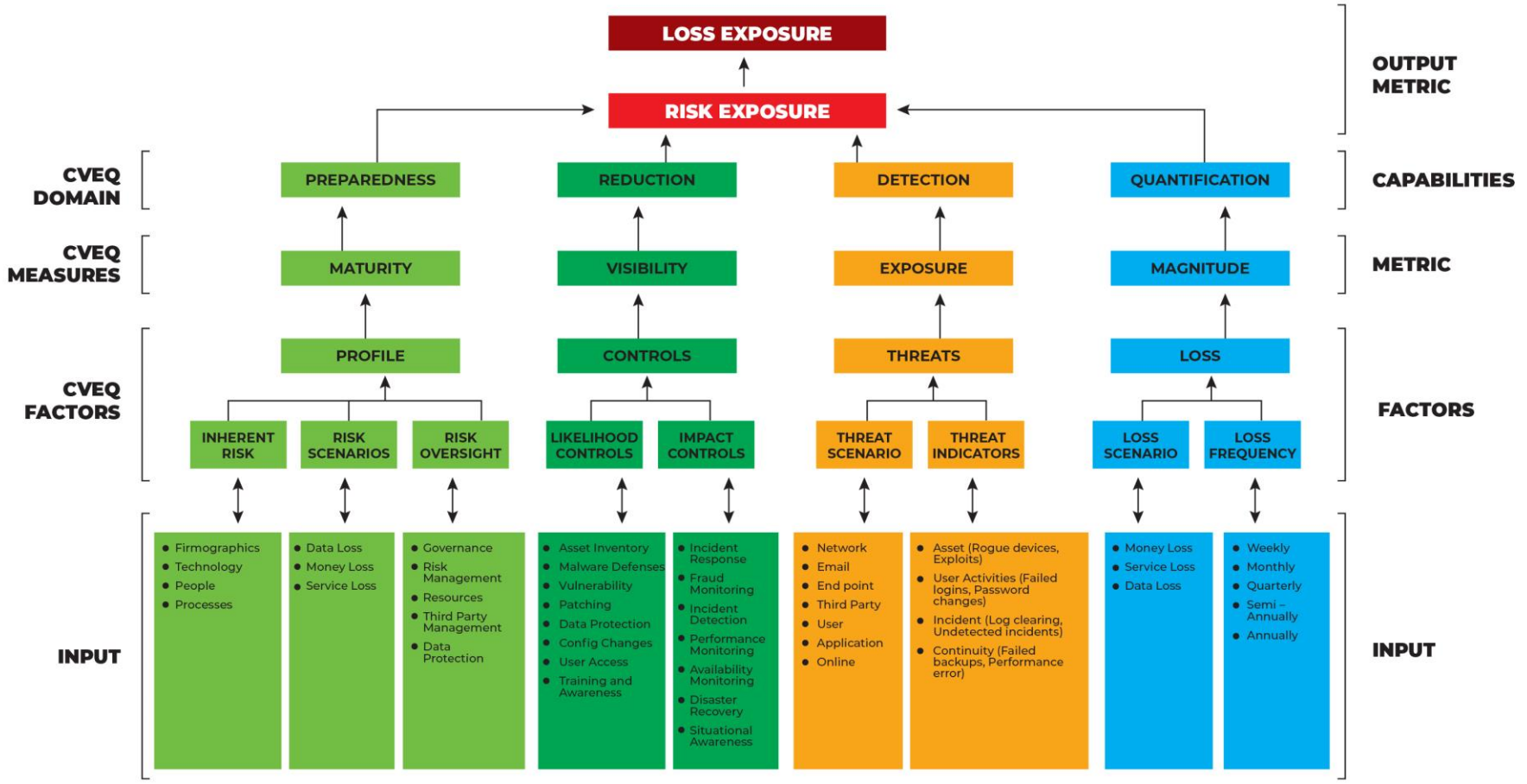
Challenges with the Threat-Focused Approach to Cyber Risk Management

- 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

RISK-EXPOSURE-FOCUSED CYBER RISK PROGRAM


HEALTH RISK EXPOSURE
HEALTH PREPAREDNESS LEVEL
HEALTH CONTROLS EFFECTIVENESS
INDICATOR LEVEL
OUTCOME LIKELIHOOD
Profile
Wellness
Morbidity
Outcome
Biometrics
Possible Outcome Scenario
Lifestyle
Physical Wellness
Mental Wellness
Disease
Symptoms
Possible Outcome Scenario
Possible Outcome Frequency
• Weight
• Age
• Height
• Sex
• Family history
• Disease
• Disability
• Death
• Nutrition
• Attitude
• Prayer
• Diet
• Personal growth
• Sleep
• Exercising
• Weight Management
• Steps
• Physical
• Therapy
• Regular checks
• Blood checks
• Diabetes
• Cancer
• Stroke
• COVID 19
• Malaria
• Fever
• Sore Throat
• Headache
• Infectious
• Deficiency
• Hereditary
• Physiological
• Daily
• Weekly
• Monthly

RISK AREA	HEALTH RISK MANAGEMENT	CYBER RISK MANAGEMENT
RISK PREPAREDNESS	Biometric (Weight, Height, Age, Sex, Family history)	Firmographic (Industry, Revenue, Geography, Size)
	Lifestyle (Nutrition, Attitude, Prayer, Diet, Personal Growth, sleep)	Oversight (Governance, Risk Management, Resources, Third Party Management, Data Protection)
RISK REDUCTION	Wellness (Physical and Medical) • physical wellness (Exercising, Weight Management, steps) vs	Controls (Likelihood and Impact) • Likelihood - (Asset, User,
	medical wellness(Physical Therapy, Regular checks, blood checks)	Impact - Incident, Continuity)
RISK DETECTION	Disease (Diabetes, Cancer, Stroke, COVID 19, Malaria)	Threats (Malware, Ransomware, Rogue Device, Insider, Espionage)
	Symptoms (Fever, Sore throat, Headache)	Threat Indicator (Failed Logon, Database modifications, performance degradation, User account deletion)
RISK QUANTIFICATION	Morbidity (Infectious, deficiency, hereditary, physiological)	Risk Exposure (Unauthorized data transfer, unauthorized data disclosure, unplanned resource unavailability, unauthorized funds transfer)
	Mortality (infectious, deficiency, hereditary, physiological)	Loss Exposure (Fraud, Sabotage, Data Loss/ Theft)



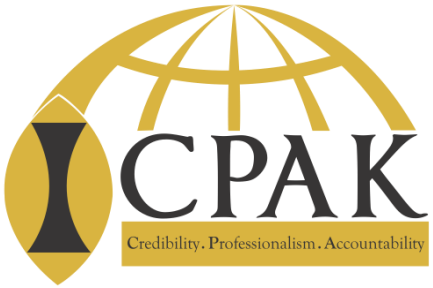
Vision: A world class Professional Accountancy Institute.

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.

Risk-based Cyber Risk Monitoring Approach



Risk	Assets	Threats	Incidents
Risk Profile	**In-Scope Processes**	**Threat Scenarios**	**Triggered Events**
High Risk (Banking) High risk activities (online channels), High risk technology (remote access)	Mobile banking process; Card management process; Electronic payment process; payroll process; Customer registration process	Network attack, application compromise, data manipulation; remote access abuse	Malware alerts from anti-virus system, Failed logins to a critical server, Communication to a malicious IP
Risk Exposure	**In-Scope Assets**	**Threat Indicators**	**Detected Incidents**
High Risk (Banking) High risk activities (online channels), High risk technology (remote access)	Mobile banking infrastucture; card payment process infrastructure; payroll management systems; Customer relation management systems	End-Point Malware; Network Traffic Malware; Communication Protocol Abuse; System File Abuse System services Abuse; registry Abuse; Malicious traffic	Malware detected on the mail server, Critical file transferred from cloud server, Firewall rule updated
Risk Scenario	**Asset Clusters**	**Monitoring Rules**	**Incident Response**
Fraud (Mobile, card, wire transfer), **Data Theft** (Employee, customer) **Sabotage** (customer portal, third party system)	Fraud exposure cluster, Data theft exposure cluster; Sabotage exposure cluster,	User fails more than three login attempts, Specific types are copied to USB drives, Sent as email attachments to non-company domains	Malware clean-up, File transfer incident investigated, Firewall rule changes reversed

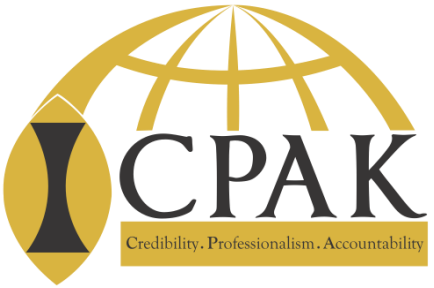
RISK-EXPOSURE-ORIENTED PROGRAM (ROC-BASED)

Vision: A world class Professional Accountancy Institute.

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



Threats	Target	Risk	Loss
Threats Actors	Target Asset	Risk Impact	Loss Exposure
Threat Actions ↓ Access ↓ Misuse ↓ Disclosure ↓ Deny access ↓ Modification ***Breach Scenarios***	Target Controls ↓ Asset Controls ↓ User Controls ↓ Incident Controls ↓ Continuity Controls ***Control Effectiveness***	Risk Events ↓ Fraud Loss of funds ↓ IP Theft Loss of data ↓ Sabotage Loss of service ***Risk Exposure***	Loss Events ↓ Revenue Loss ↓ Remediation Loss ↓ Productivity Loss ↓ Reputation Loss ↓ Fines and Legal Loss ***Loss Expectancy***
Threat Intelligence, Research and Trends, Analytics, Big Data	Analytics, Technology, Processes, Automation, Awareness, Orchestration, Monitoring	Analytics, Quantification, Aggregation, Automation	Cyber Insurance, Quantification, Analytics
CBEST, TIBER-EU, MITRE, SAMA CSF	**ISO 27001, NIST, COBIT, CMMC, CIS Controls, GDPR**	**NIST SP 800-30, RiskIT, FFIEC CAT, MIT SCRAM, CVEQ**	**FAIR, CVEQ, CDM, BITSIGHT, MARSH, FICO, CORAX**

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

Step by Step Approach to Developing a Cyber Risk Program

- Strategic shift from "**Seeking to detecting threats**" "Seeking to reducing Exposure"
- ERM/Business integration of cyber security issues
- Streamline "Cyber risk models" vs "Extensive" cyber security frameworks

IMPLEMENTING THE RISK-EXPOSURE CYBER RISK PROGRAM (STEP BY STEP IMPLEMENTATION GUIDANCE)

Risk Preparedness (Maturity)

- **Operational Profile-** Have you identified and prioritized a listing of key operational activities that generate value for your organization?
- **Digital Profile-** Have you identified and prioritized a listing of top digital-enabled processes and assets that create value for your organization?
- **Inherent Risk -** Have you assessed and determined the level of digital risk posed to the organisation by its digital assets and processes?
- **Risk Oversight Maturity -** Have you assessed and determined the maturity level of risk management and monitoring structures established by the organizations leadership?
- **Risk Maturity Profile -** Have you analyzed and determined if the organizations risk oversight maturity levels adequately matches the inherent risk level?
- **Risk Capacity -** Have you analyzed and determined the maximum level of risk that your organization can handle based on the inherent risk profile?
- **Risk Appetite -** Have you analyzed and determined the level of risk that your organization is willing to accept in pursuit of its objectives based on the inherent risk profile?
- **Risk Exposures -** Have you identified and prioritized your top cyber risk exposures and threat scenarios?
- **Risk Treatment Options-** Have you identified and prioritized your top inherent risk treatment initiatives?
- **Risk Profile Reporting -** Have you identified and communicated the organizations inherent risk profile to key stakeholders?

Risk Reduction (Visibility)

- Refers to the ability of an organization to implement controls and countermeasures that effectively and aggregately reduce or minimize the likelihood of an organizations cyber risk exposure.
- The risk reduction capability enables an organization to consistently implement and measure the effectiveness of controls
- It seeks to answer the following five questions:
  1. What is the control effectiveness of existing asset-related risk reduction measures? (Malware, configuration changes, vulnerability controls, inventory and data protection controls)
  2. What is the control effectiveness of user-related risk reduction measures? (Privileged access, user/identity access management, user awareness and training)
  3. What is the control effectiveness of incident-related risk reduction measures?(Transaction monitoring, incident response, Monitoring and analysis)
  4. What is the current capability and effectiveness of continuity-related risk reduction measures? (Disaster recovery, performance and availability monitoring)
  5. What is the overall risk reduction capability and aggregate effectiveness of implemented Controls?

Risk Reduction (Visibility)

- **Control Framework -** Have you identified and prioritized a set of practices, procedures and technologies intended to minimize risk in a coordinated manner?
- **Control Design -** Have you designed and implemented risk countermeasures or control to reduce the likelihood or impact of identified risk exposures?
- **Control Operation -** Have you identified and implemented performance indicators to ensure the continuing effectiveness of implemented controls?
- **Control Effectiveness -** Have you analyzed and measured the aggregate capability and effectiveness of implemented risk controls ?
- **Control Deficiencies -** Have you identified and prioritized weakness or failures in the capabilities or effectiveness of implemented controls?
- **Residual Risk Profile -** Have you identified and prioritized your top residual risk exposures based on the organisations control deficiencies?
- **Risk Tolerance Level -** Have you analyzed and determined the level of residual risk acceptable to your organization based on identified control deficiencies and residual risk profile?
- **Risk Remediation Plan -** Have you identified and prioritized a listing of key actions and initiatives that are likely to reduce the impact or likelihood of a residual risk exposure?
- **Risk Reduction Impact -** Have you analyzed and quantified the impact of the remediation initiatives in reducing the likelihood of risk occurring and monetary savings – ROI?
- **Control Deficiency Reporting -** Have you identified and communicated the organizations risk profile to key stakeholders?

Risk Detection (Threat Exposure)

- Refers to the ability of an organization to effectively monitor, detect and respond to cyber threats.
- The cyber risk detection capability enable an organization to identify and prioritize relevant threat scenarios and indicators to implement in their threat monitoring process.
- It seeks to answer the following five questions:
  1. What are our top cyber threat scenarios?(Network, Email, End-point, Third Party, Online or Users)
  2. What are our top cyber threat indicators? (Assets, Users, Incident or Continuity)
  3. What is maturity and effectiveness of threat data management processes? (Mature, immature or non-existent)
  4. What is the maturity and effectiveness of the incident detection, prioritization, scalation and response processes? (Mature, immature and non-existent)
  5. What is the aggregated level of malicious activity in an organisation based on the severity of detected incidents and the criticality or sensitivity of the targeted assets? (Low, minimal, moderate, high or extreme)

Risk Detection (Threat Exposure)

- **Cyber Risk Exposures -** Have you identified and prioritized your top cyber risk exposures?
- **Cyber Threat Scenarios -** Have you identified and prioritized your cyber threat scenarios?
- **Cyber Threat Indicators -** Have you identified and prioritized your cyber threat indicators?
- **Threat Data Sources -** Have you identified and validated your sources of threat data?
- **Threat Data Aggregation -** Have you collected and aggregated cyber threat data?
- **Threat Data Correlation -** Have you cleansed and correlated cyber threat data?
- **Threat Indicator Analysis-** Have you identified and implemented a process to incident monitoring rules and use cases?
- **Incident Escalation Process -** Have you developed and implemented an incident escalation process?
- **Incident Response Plan -** Have you developed and implemented an incident response plan?
- **Threat Exposure Reporting -** Have you identified and communicated the organizations threat exposure to key stakeholders?

Risk Quantification (Loss Magnitude)

- Refers to the ability of an organisation to use mathematical modeling techniques to accurately represent the organizations cyber risk posture.
- Risk Quantification provides the organization with a clear snapshot of its potential losses in monetary terms. This enables an organisation to prioritize its cyber risk mitigation and management efforts.
- It seeks to answer the following five questions:
  1. What is the organizations top cyber risk exposures (loss of data, loss of service or loss of funds)
  2. What is the organizations risk exposure level (risk profile level, control deficiency level and threat exposure level)
  3. What is the organizations top cyber loss exposure scenarios (revenue loss, remediation costs, productivity loss, reputation loss, fines and legals)
  4. What is the organizations annualized loss exposure amounts (magnitude and frequency)
  5. What is the organizations loss tolerance level (high, medium or low)

Risk Quantification (Loss Magnitude)

- **Risk Profile Scoring-** Have you analyzed and quantified your cyber risk preparedness capability?
- **Control Deficiency Scoring -** Have you analyzed and quantified your risk reduction capability?
- **Threat Exposure Scoring -** Have you analyzed and quantified your cyber risk detection capability?
- **CVEQ Risk Scoring -** Have you analyzed and quantified your risk reduction capability?
- **Risk Scenarios -** Have you identified and prioritized your residual risk scenarios?
- **Loss Scenarios -** Have you identified and prioritized your top loss scenarios?
- **Loss Data Analysis** - Have you identified and analyzed historical cyber loss data relevant to the risk scenarios in your organization?
- **Loss Expectancy -** Have you analyzed and quantified your organizations estimated annualized loss expectancy?
- **Loss mitigation -** Have you assessed and prioritized loss mitigation initiatives?
- **Loss Expectancy Reporting -** Have you identified and communicated the organizations annualized loss expectancy exposure to key stakeholders?

CONCLUSION

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*

Communicating Cyber Risk in Financial Terms

How does our actual risk compare to our risk appetite?

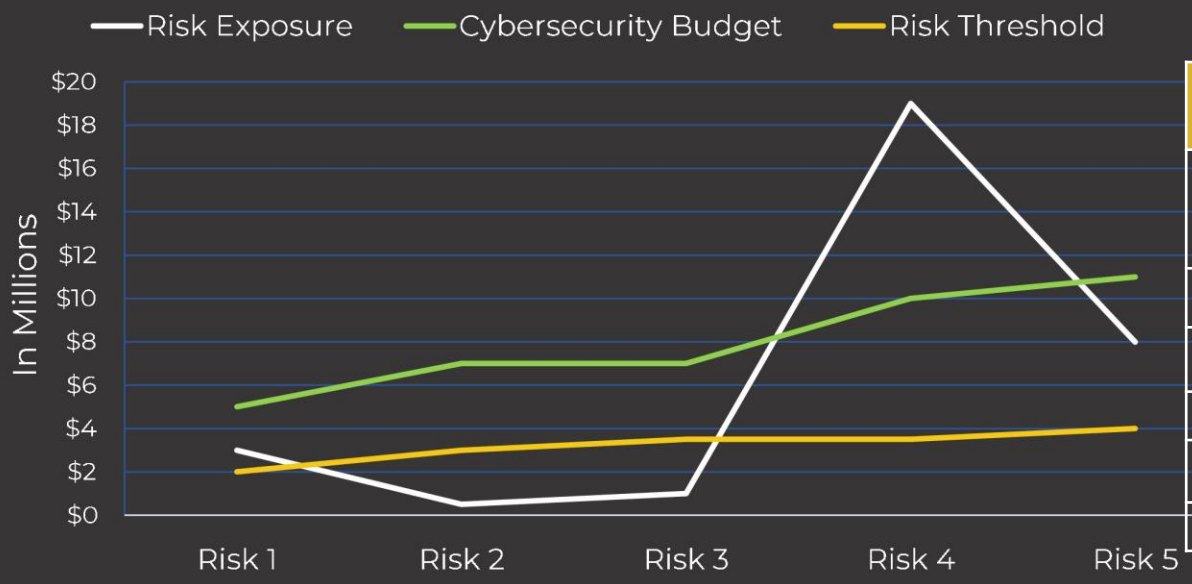
What assets represent the greatest risk exposure?

Did risk decline or increase in the last quarter?

What prcentage of aggregate loss exposure is driven by ehat control deficiency?

Cyber Risk Quantification – Sample Report

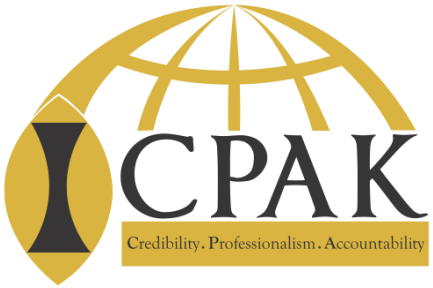
THE TOP 5 CYBER RISKS IN FINANCIAL TERMS



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

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** • Market price volatility	**Probability of default** • Economic conditions • Credit ratings	**Probability of breach** • Threat vectors • Preventative controls
SEVERITY	**Holding period** • Market liquidity of investments	**Loss in the event of default** • Collateral rights • Bankruptcy rights	**Loss in the event of breach** • Dwell time • Resolution time • Detective, mitigation and proactive controls
CORRELATION	**Price correlations** • Asset allocation • Position concentrations	**Default correlations** • Loan concentrations • Country/ industry diversification	**Threat/ control correlations** • Cyber attack patterns • Central points of failure: IT infrastructure, supply chain



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.