

Transforming Cyber Risk Management: A Case for Risk Modelling and Combined Cybersecurity Assurance



The Institute of
Internal Auditors



S E R I A N U



CVEQ™
Framework

Objectives

- Introduction
- Industry Trends and Insights
- Threat vs Risk-Focused Approach
- Red Team vs Blue Team Approach
- Combined Assurance – A Purple Team Approach
- Conclusion



The Institute of
Internal Auditors





INTRODUCTION

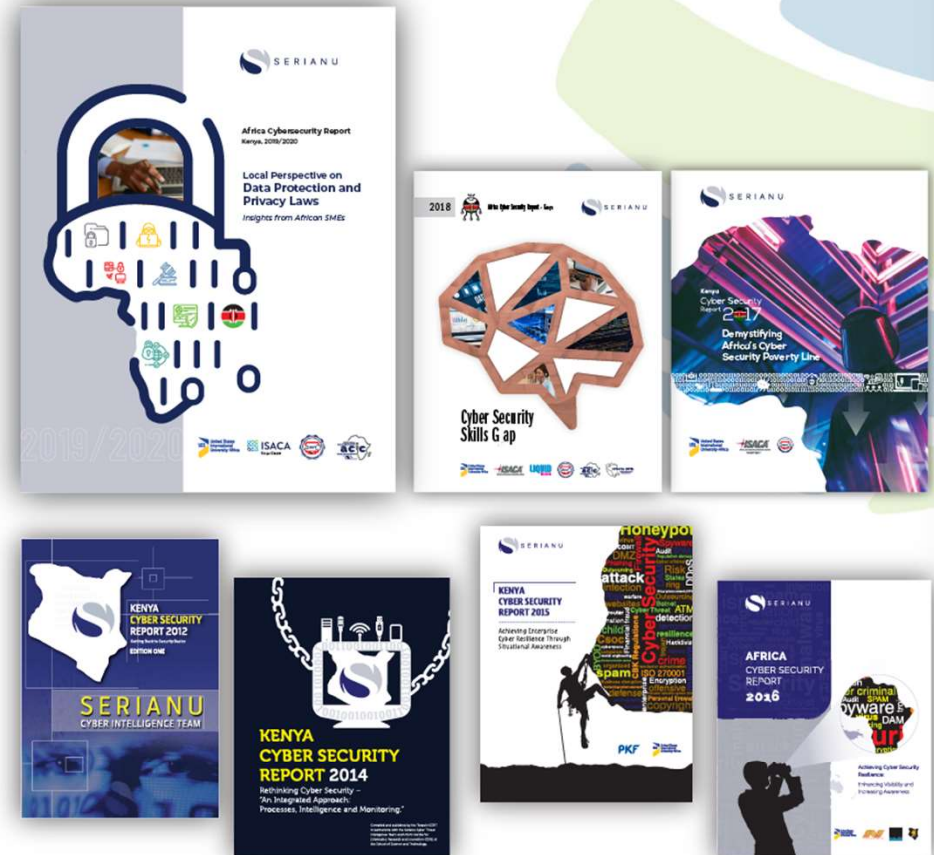


About Serianu

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



24/7 Cyber Security Centre



The Institute of
Internal Auditors



SERIANU



CVEQ™
Framework

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.

INDUSTRY TRENDS AND INSIGHTS



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

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.



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.

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.

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.

Q2: 2020



The Institute of
Internal Auditors





- **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.**



The Institute of
Internal Auditors



Threat Scenarios



Phishing



Denial of Service



Remote Access Attacks



Third Party Attacks



Malware Distribution



Exploitation of new teleworking infrastructure



Business Email Compromise



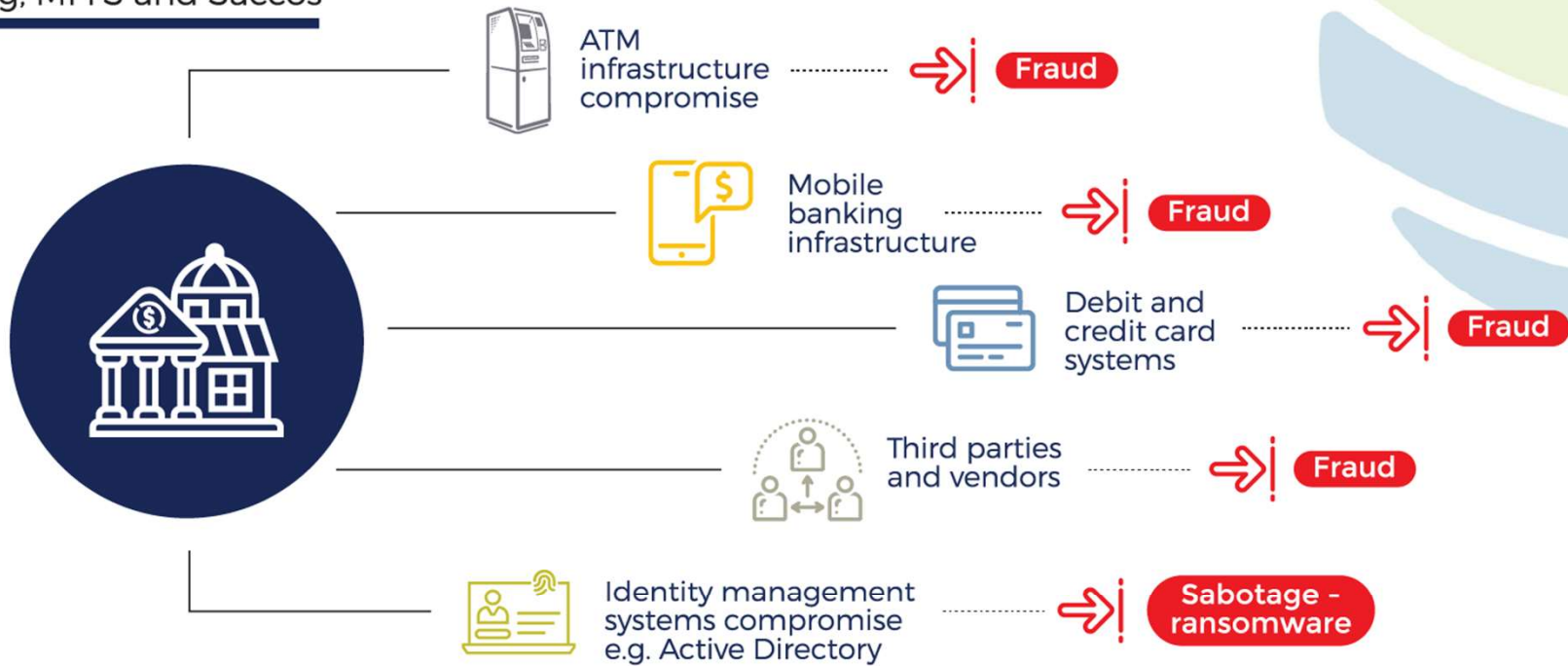
Ransomware



The Institute of
Internal Auditors

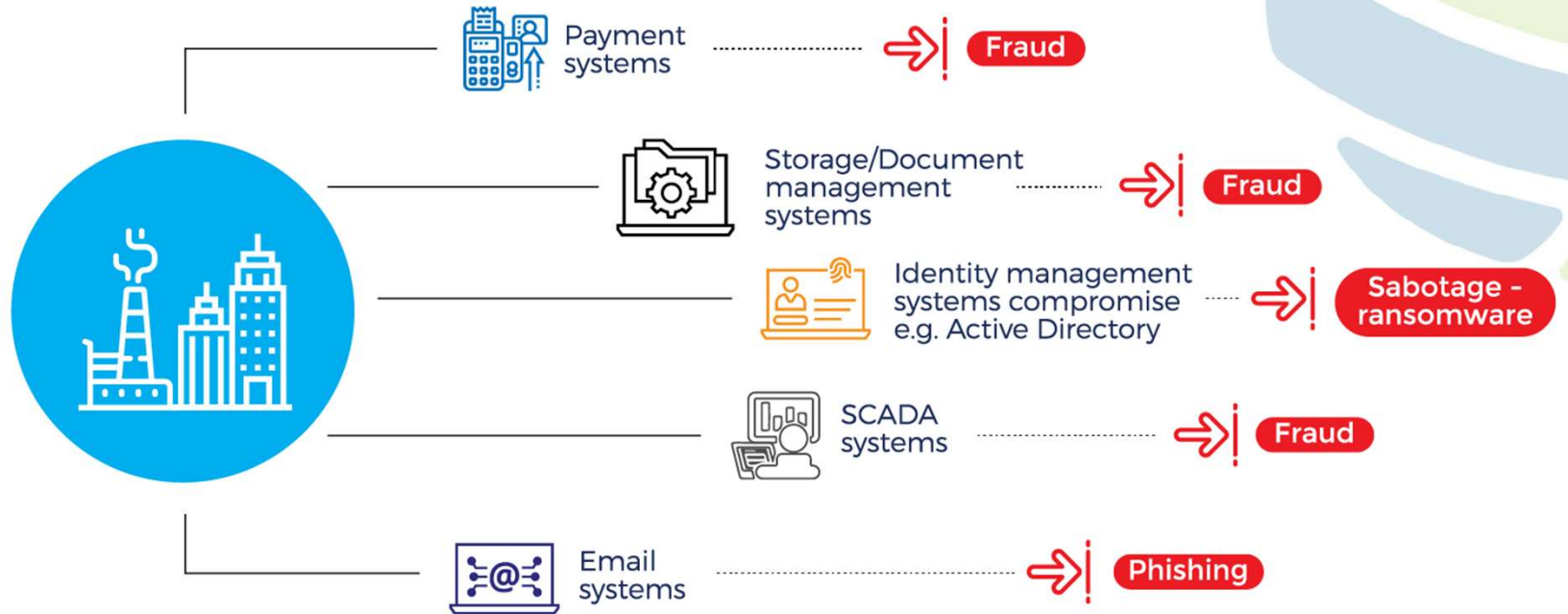


Financial Sector:
Banking, MFI'S and Saccos



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 • NGO's/Non-profit

Challenges Facing African Organizations

- 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 ASSURANCE



Traditional Cyber Risk Management Approach

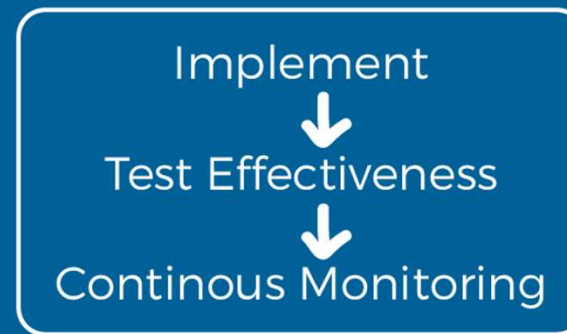
THREAT-BASED CYBER RISK MANAGEMENT PROGRAM

Risks



Register

Controls



Audit Report

Threat-Exposure-Oriented Program (SOC-Based)



The Institute of
Internal Auditors



Characteristics of Threat-Focused Approaches to Cyber Risk Management

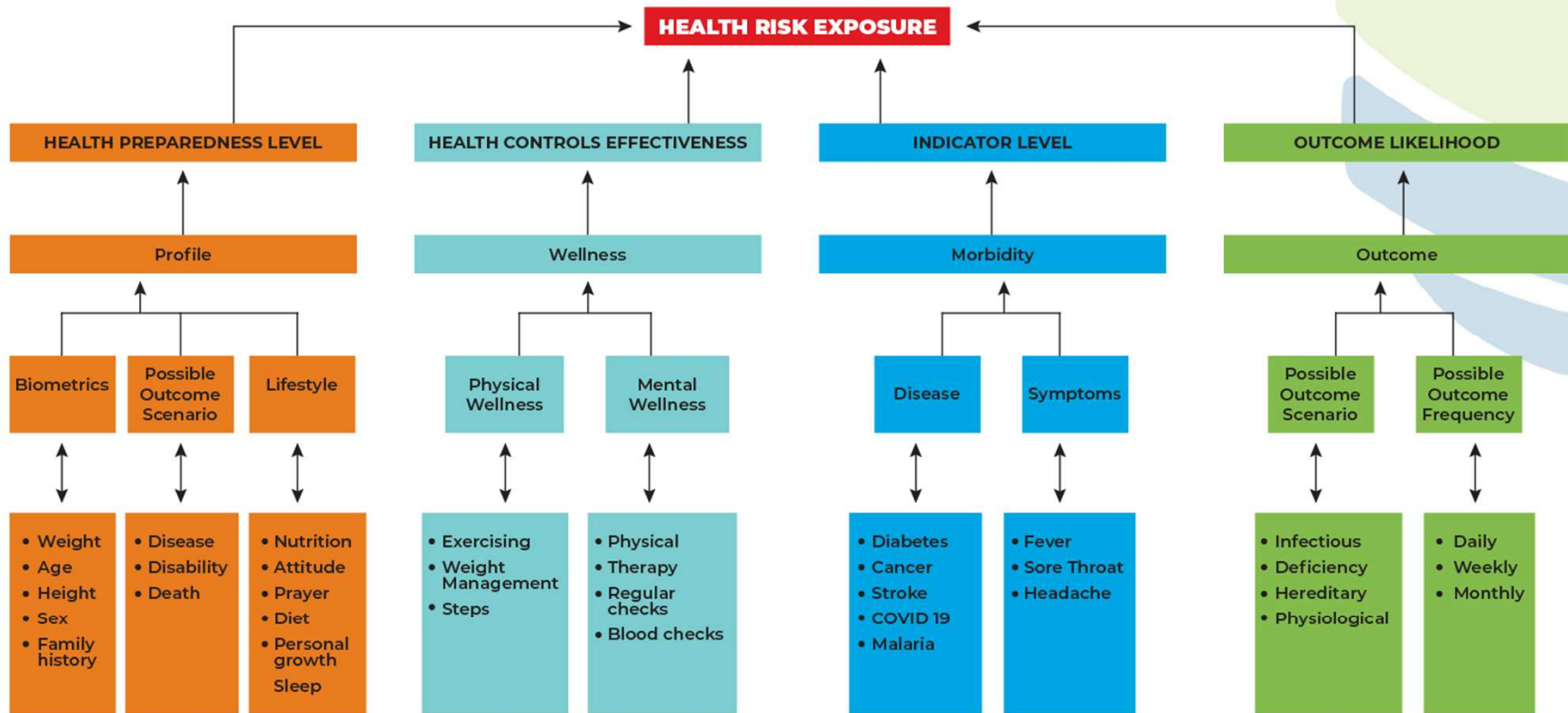
- Reactive – based on identified incidents
- Too Technical – lack of business risk perspective
- Siloed- focuses on technology vulnerabilities
- Irregular risk audits – lack of integration to risk profiling process
- Manual and tedious – the mitigation strategy is tedious and not efficient

Challenges with the Threat-Focused Approach to Cyber Risk Management

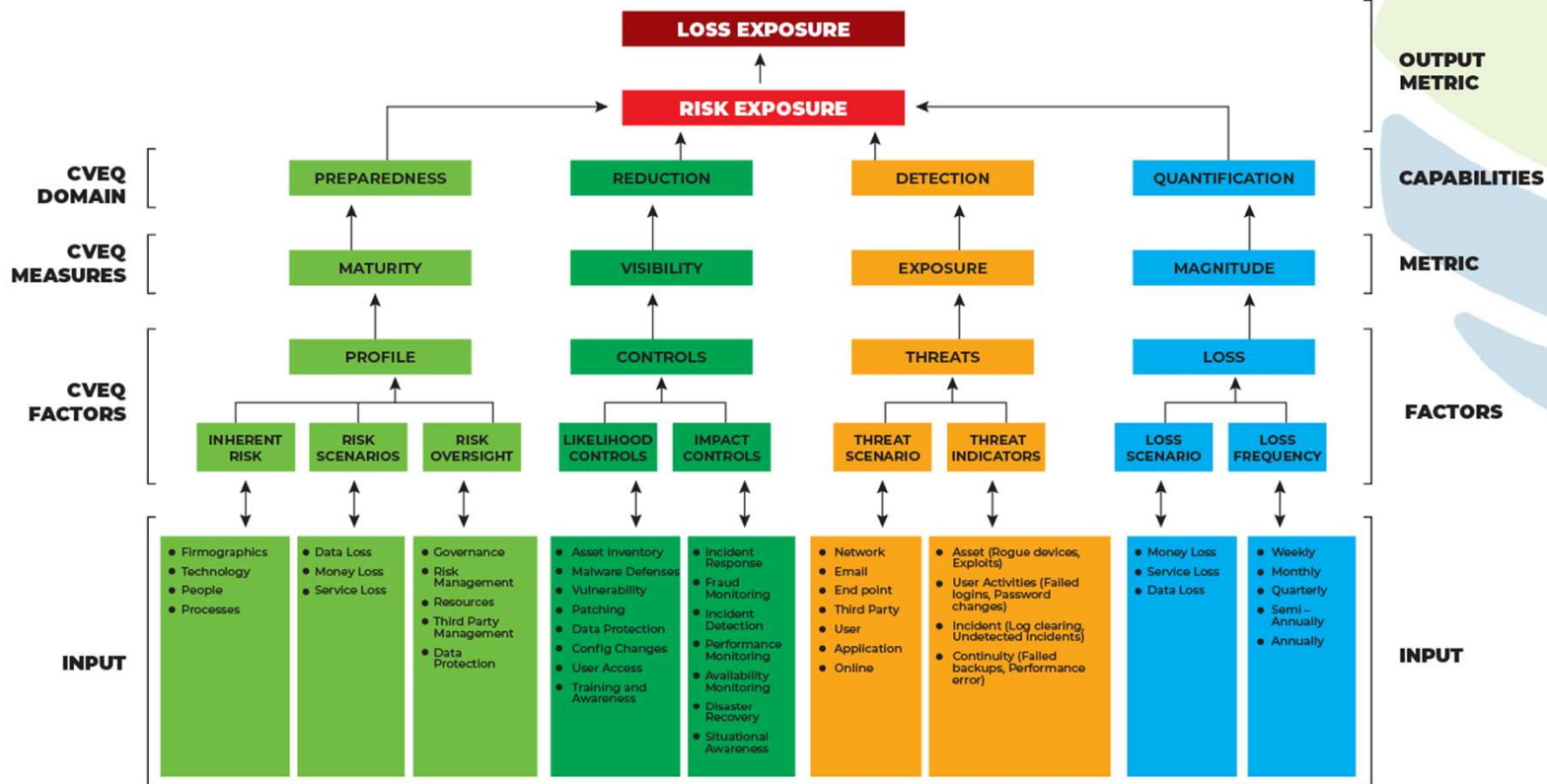
- Lack of standardized measures
- Lack of Asset information
- Informal Analysis Methods
- Focus on system level vs business level - credit risk, market risk,
Cyber risk??
- Increasing system and Ecosystem Complexity - Cloud and 3rd parties

RISK-EXPOSURE-FOCUSED CYBER RISK ASSURANCE





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



Emerging Approaches to Cyber Risk Management

Organizations 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 MANAGEMENT PROGRAM




RISK-EXPOSURE ORIENTED PROGRAM (ROC-BASED)

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

RED TEAM vs BLUE TEAM SECURITY ASSURANCE APPROACH



Red Team vs Blue Team

- **Red teams** are offensive security professionals who are experts in attacking systems and breaking into defenses.
- **Blue teams** are defensive security professionals responsible for maintaining internal network defenses against all cyber attacks and threats.
- **Red teams simulate attacks** against blue teams to test the effectiveness of the network's security.
- These **red** and **blue** team exercises provide a holistic security solution ensuring strong defenses while keeping in view evolving threats.

Typical team responsibilities

Red Team	Blue Team
<ul style="list-style-type: none">• Vulnerability Scanning• Social Engineering• Physical and Digital Pentesting (typically done in a vacuum)• Open-source intelligence gathering	<ul style="list-style-type: none">• Threat intelligence• Malware and exploit reverse engineering• Digital Forensics• Active Monitoring

What is a Red Team?

- A red team consists of security professionals who act as adversaries to overcome cyber security controls.
- Red teams often consist of **independent ethical hackers** who evaluate system security in an objective manner.
- They utilize all the available techniques to find weaknesses in people, processes, and technology to gain unauthorized access to assets.
- As a result of these simulated attacks, red teams make recommendations and plans on how to strengthen an organization's security posture.



Examples of Red Team Exercises

- **Penetration testing**, also known as ethical hacking, is where the tester tries to gain access to a system, often using software tools. For example, 'John the Ripper' is a password-cracking program. It can detect what type of encryption is used, and try to bypass it.
- **Social engineering** is where the Red Team attempts to persuade or trick members of staff into disclosing their credentials or allowing access to a restricted area.
- **Phishing** entails sending apparently-authentic emails that entice staff members to take certain actions, such as logging into the hacker's website and entering credentials.
- **Intercepting communication software tools** such as packet sniffers and protocol analyzers can be used to map a network, or read messages sent in clear text. The purpose of these tools is to gain information on the system. For example, if an attacker knows a server is running on a Microsoft operating system then they would focus their attacks to exploit Microsoft vulnerabilities.
- **Card cloning** of an employee's security card to grant access into unrestricted areas, such as a server room.

What is a Blue Team?

- A blue team consists of security professionals who have an inside out view of the organization.
- Their task is to protect the organization's critical assets against any kind of threat.
- They are well aware of the business objectives and the organization's security strategy.
- Therefore, their task is to strengthen the castle walls so no intruder can compromise the defenses.

Examples of blue team exercises

- Performing DNS audits (domain name server) to prevent phishing attacks, avoid stale DNS issues, avoid downtime from DNS record deletions, and prevent/reduce DNS and web attacks.
- Conducting digital footprint analysis to tracks users' activity and identify any known signatures that might indicate a breach of security.
- Installing endpoint security software on external devices such as laptops and smartphones.
- Ensuring firewall access controls are properly configured and that antivirus software are kept up to date
- Deploying IDS and IPS software as a detective and preventive security control.
- Implementing SIEM solutions to log and ingest network activity.
- Analyzing logs and memory to pick up unusual activity on the system, and identify and pinpoint an attack.
- Segregating networks and ensure they are configured correctly.
- Using vulnerability scanning software on a regular basis.
- Securing systems by using antivirus or anti-malware software.
- Embedding security in processes.



Benefits of a Blue vs Red Team Strategy

- ❑ Implementing a red and blue team strategy allows an organization to benefit from two totally different approaches and skillsets.
- ❑ It also brings a certain amount of competitiveness into the task, which encourages high performance on part of both teams.
- ❑ The red team is valuable, in that it identifies vulnerabilities, but it can only highlight the current status of the system.
- ❑ On the other hand, the blue team is valuable in that it gives long term protection by ensuring defenses remain strong, and by constant monitoring of the system.
- ❑ The key advantage, however, is the continual improvement in the security posture of the organization by finding gaps and then filling those gaps with appropriate controls.
- ❑ .

COMBINED ASSURANCE - A PURPLE TEAM APPROACH



How Do Red And Blue Teams Work Together?

- ❑ When the test is complete both teams gather information and report on their findings.

- ❑ The red team advises the blue team if they manage to penetrate defenses, and provide advice on how to block similar attempts in a real scenario.

- ❑ Likewise, the blue team should let the red team know whether or not their monitoring procedures picked up an attempted attack.

- ❑ Both teams should then work together to plan, develop, and implement stronger security controls as needed.

What is a Purple Team

- ❑ While red teams and blue teams share common goals, they're often not politically aligned.
- ❑ When Red teams who report on vulnerabilities are praised for a job well done.
- ❑ They're not incentivized to help the blue team strengthen their security by sharing information on how they bypassed their security.
- ❑ The goal of a purple team is to bring both red and blue teams together while encouraging them to work as a team to share insights and create a strong feedback loop.
- ❑ Enhanced cooperation between both teams through proper resource sharing, reporting and knowledge share is essential for the continual improvement of the security program.

Current State

- ❑ **Red** and **Blue** Team often operate in a vacuum on a day-to-day basis, sometimes even within their own teams
- ❑ Feedback loops consist of reports being tossed over the wall if shared at all
- ❑ Emphasis is given on remediation of vulnerabilities rather than prevention and detection growth
- ❑ Teams are incentivized by their ability to outwit the other side
- ❑ Red Team are often composed at least partially of outsourced groups



Team Structure and Incentives

Misaligned Incentives

Red Team	Blue Team
<ul style="list-style-type: none">• Big scary report = job well done• Success is dependent on how many controls the team can bypass (Blue team failure points)	<ul style="list-style-type: none">• No alerts = preventative controls all worked!• A lot of alerts means that detection capabilities are firing on all cylinders



Feedback Loops

How'd you do that?

- ❑ Team paring:
 - ❑ Allow the Blue Team to see how things work:
 - Exploits
 - Pivoting
 - Credential harvesting
 - Allow the Red Team to see how things work:
 - Active monitoring and alerts
 - Response playbook
 - Policies
- ❑ What are the specific forensic artifacts from all of the above?
- ❑ Do we understand why these attacks are succeeding?

Can you see me now?

- ❑ During vulnerability scans and more in-depth exploit attempts:
 - Does the Blue Team have logs of all attack activity?
 - Are alerts set up for successful or continued attempts?
 - Does the Blue Team know how to query logs for attack activity?
 - What is the response procedure for the various scans and attacks that are attempted?
- ❑ Each of the above represent a potential gap that can be improved upon
- ❑ This can occur for all parts of an organization (corporate network, product, badging systems, employee workstations, etc.)

Red Team vs Blue Team Metrics

Red Team Metrics

- Attack complexity
- Number of targets
- Duration of exercises
- Boxes compromised
- Users compromised
- Historical data

Blue Team Metrics

- Attacks Detected
- Detection Time
- Response Time
- Forensic Information
- Improvement from Previous Tests

Purple Team Metrics

- ❑ Measure improvement scan over scan
- ❑ Measure growth in team knowledge
 - Red Team learning Blue Team playbook
 - Blue Team learning Red Team TTPs

Apply It



What should you apply?

Proactive protection

- Risk Scenarios
- Risk Modeling
- Tabletop exercises
- Threat modeling
- Security assessments

CONCLUSION



Step by Step Approach to developing a Cyber Risk Program

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

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*



Our Contacts

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