SERIANU

Assessing the Performance and Effectiveness of Cyber Security Controls

Brought to you by

Serianu Cyber-Threat Command Centre

Cyber Immersion Clubs

24/7 Cyber security command Centre – KE and *BW – Aug 2019*

SERIANU

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.

OVERVIEW

OVERVIEW

- The Cyber security problem
- Current State of Cyber security in Organizations
- Challenges with the current approach
- The future of Cyber security Management
- The 7 layers of cyber risk exposure management

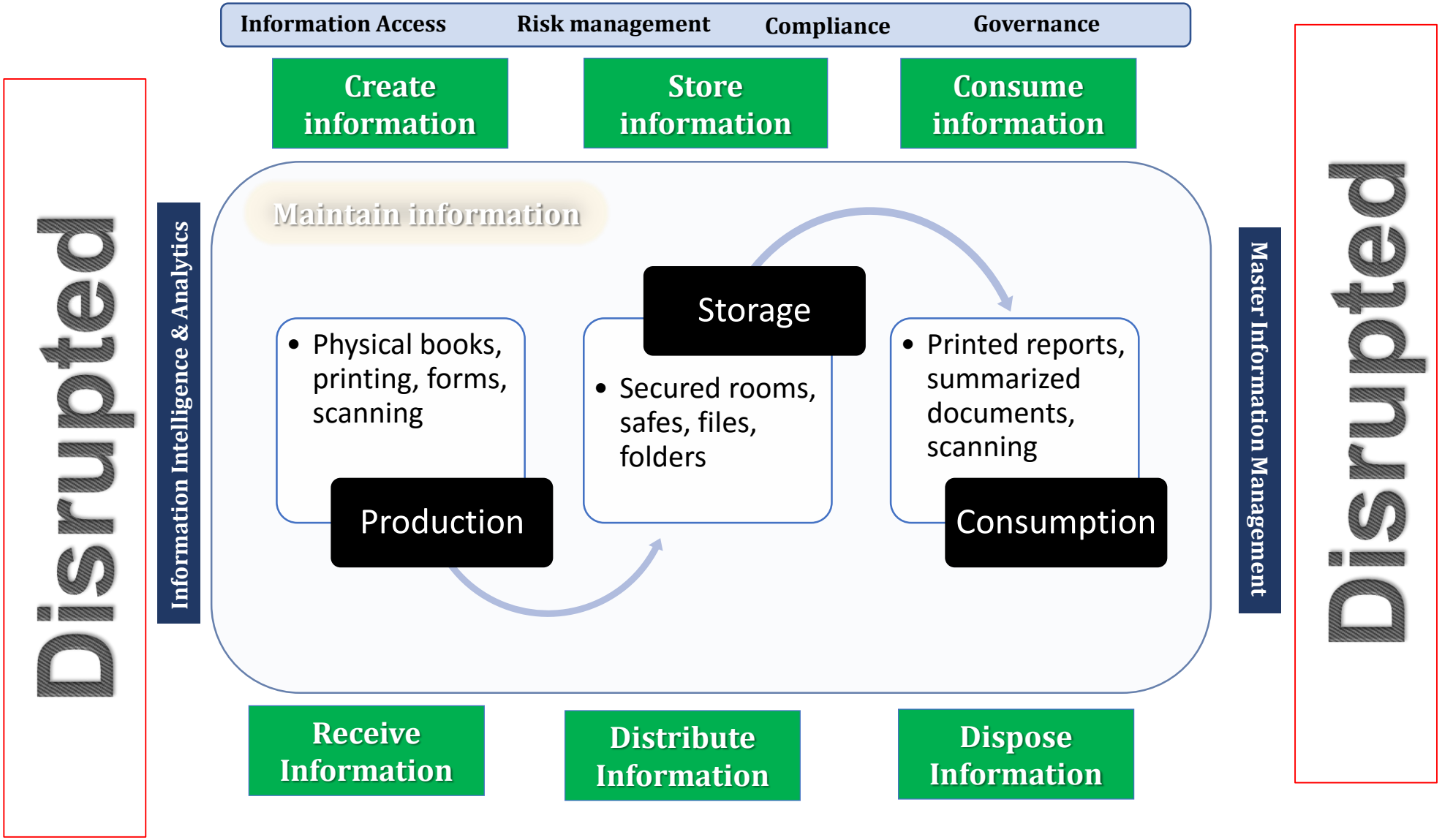
OVERVIEW

OVERVIEW

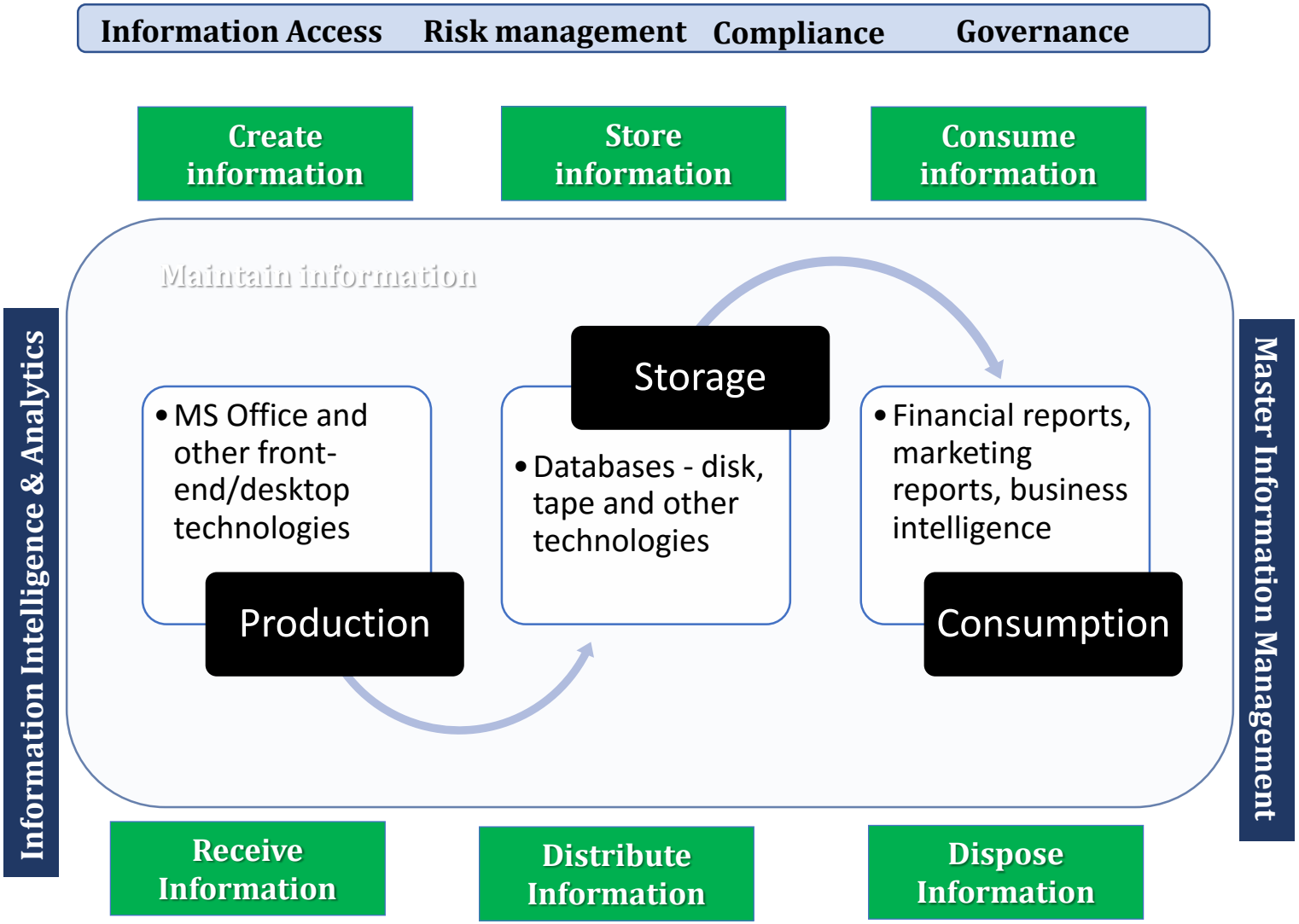
- The Cyber security problem
- Current State of Cyber security in Organizations
- The Problem with the current state
- The future of Cyber security Management
- The 7 layers of cyber risk exposure management

The Cybersecurity Problem in Africa

Non-digital – Information Lifecycle Management



Digital – Information Lifecycle Management



The Cybersecurity Problem

- ✓ Understand
- ✓ Attribution
- ✓ Deterrence

Understanding

Understanding the anatomy and basis of cyber attacks

- Network Monitoring
- Detective controls
- Preventive controls
- Risk Program
- Visibility

Understanding

Collecting evidence, build timelines and gathering evidence in the wake of a cyber attack.

- ❑ Forensics
- ❑ Collaboration
- ❑ Standards
- ❑ Investigation

Deterrence

Deterrence is a strategy to dissuade or prevent adversaries from taking specific malicious actions. This can be gained through:

- ❑ Laws and policies
- ❑ Prosecution
- ❑ Investigation
- ❑ Cyber-threat Intelligence

SERIANU

2019 Cyber security priorities

OVERVIEW

OVERVIEW

- The Cyber security problem
- Current State of Cyber security in Organizations
- The Problem with the current state
- The future of Cyber security Management
- The 7 layers of cyber risk exposure management

Current state of cyber security in Corporate Africa

Risk Management	Controls Management	Audit and Compliance Management
Risk assessments	Controls Implementation – FW/AV	Audit Programs - VAPT
Risk Register – Top/Medium/Low	Infosec Programs – SOCs/Ops/Tech	Audit reports Internal/External

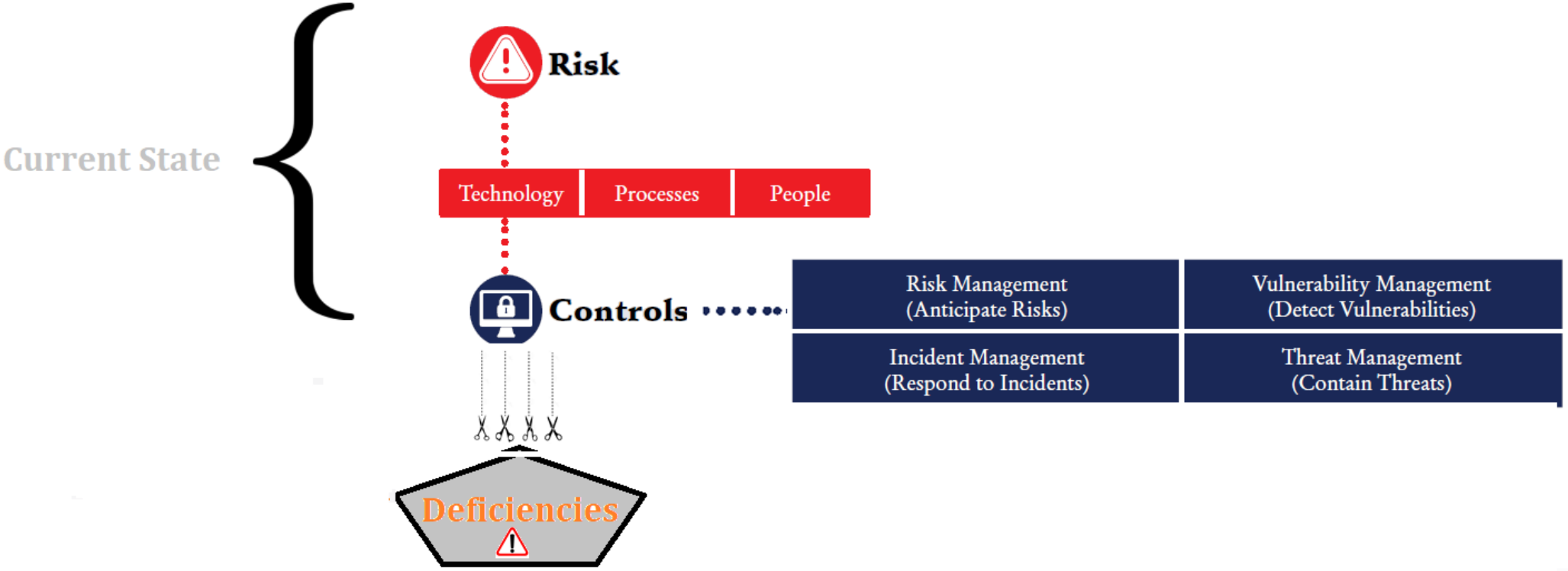
SERIANU

OVERVIEW

OVERVIEW

- The Cyber security problem
- Current State of Cyber security in Organizations
- The Problem with the current state
- The future of Cyber security Management
- The 7 layers of cyber risk exposure management

Deficiency reporting – audit reports



Using control deficiencies as a measure of our cyber security problems

- Leads to unnecessary investments in irrelevant technologies and tools
- Focusing on controls more than visibility and exposure
- Conducting annual reviews when most processes are now real-time

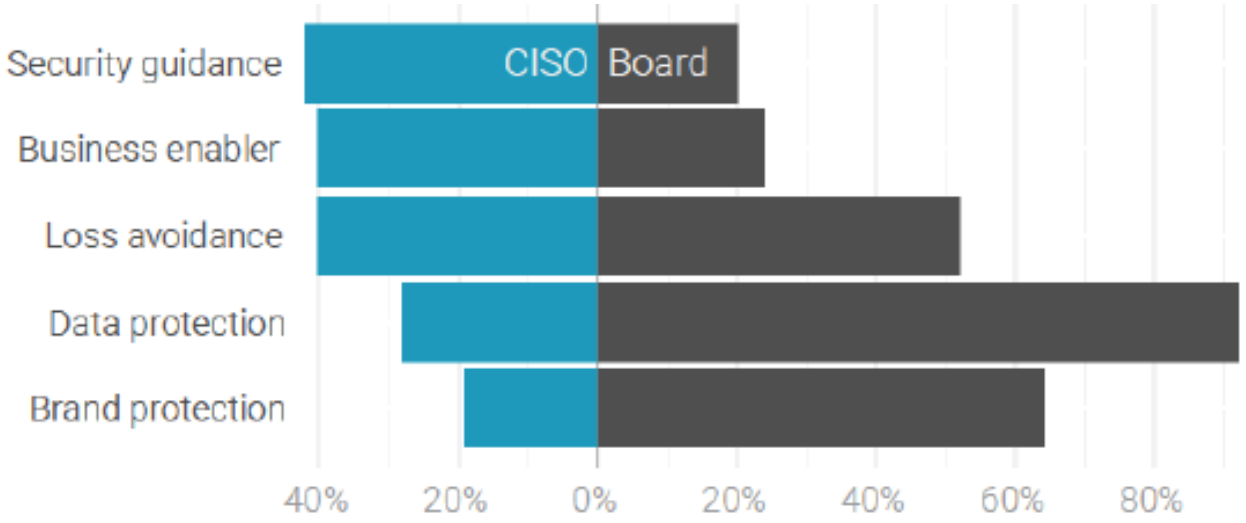
SERIANU

Perspectives from the Boardroom

Perspectives from the Board Room – 2018 Research survey

1. What is reported to the board?
2. How is it reported (e.g., format, context)?
3. Why is it reported?
4. How is it viewed by directors and other non-security execs?
5. How does all of the above differ among different types of orgs?

What is the primary value of cybersecurity to the business?



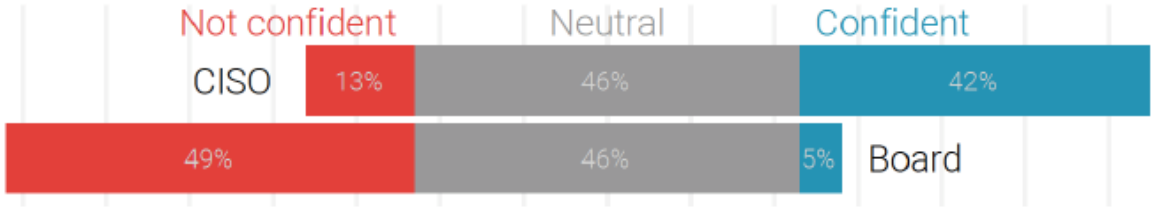
CISO PERSPECTIVE

"If I asked the Board, what my most important job is, they would say, 'Don't get breached.' But they get most upset when I didn't respond promptly to vendor/customer inquiries."

BOARD PERSPECTIVE

"Trust is the #1 value security offers to the business. Trust that we can continue to do business without major breaches or disruptions."

Are you confident with the security program's effectiveness?



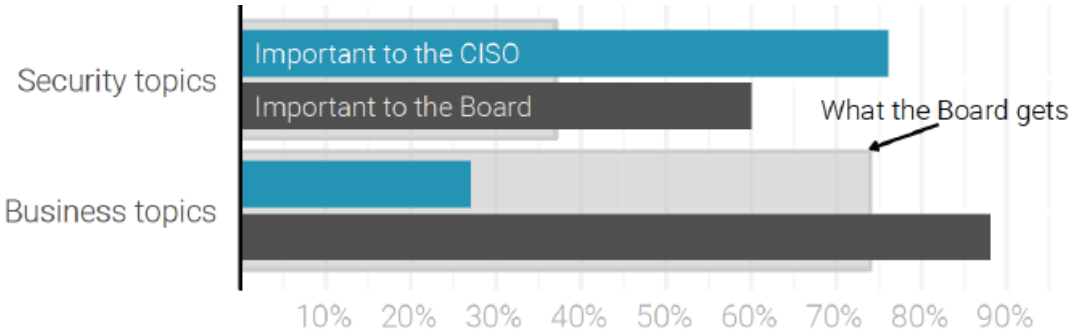
CISO PERSPECTIVE

"Several items are red at the moment. Not necessarily because they are high priority, but because there is a real risk. Green would make the Board ignore it."

BOARD PERSPECTIVE

"Directors come away with the overwhelming impression that no matter how much money they spend on security they're still going to get breached."

What metrics are reported to the Board?



CISO PERSPECTIVE

"We had a weekly metrics report that mostly useless when I cam. I stopped it, but don't know what to replace it with. I don't think the industry knows what a successful security program looks like to measure against it."

BOARD PERSPECTIVE

"Stop talking about security. Talk about the outcomes of security. Does this help the business? Does it make my life better? Does it make my life better? What do we get that we didn't before? What do we eliminate that we had before?"

SERIANU

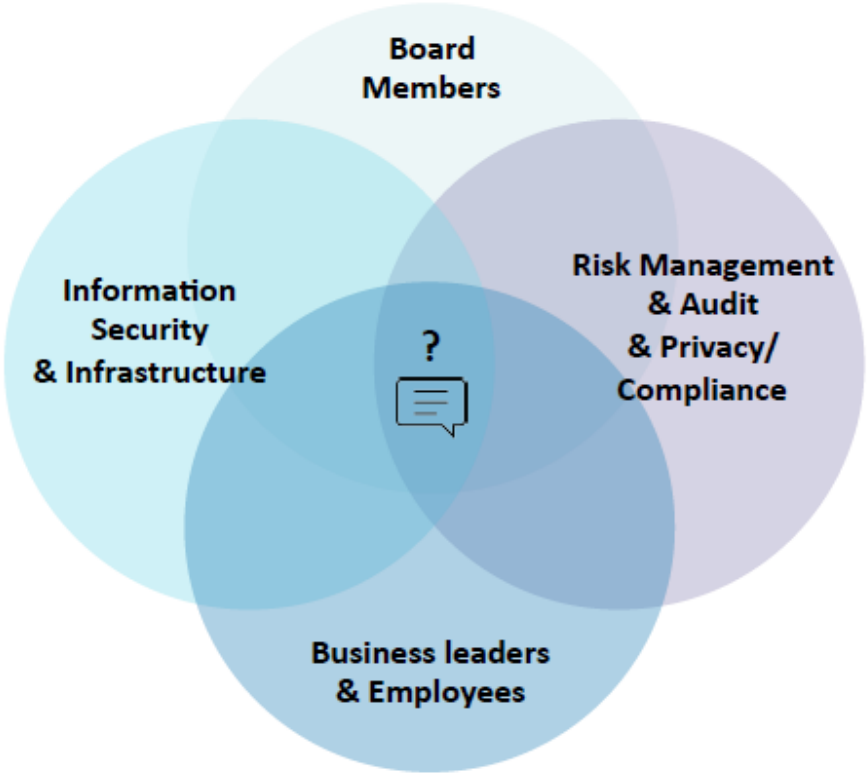
Insights from the Boardroom

Boards tend to have **SIX** key questions:

- How much cyber insurance should I buy?
- Which of our cyber risk management options are likely to be most cost-effective?
- How much risk is associated with…?
- What benefit are we getting for our current cyber risk management expenditures?
- How much cyber risk do we think we have and what is it from?
- How much less (or more) risk will we have if…?

The questions are not complicated but, are difficult to answer in simple, consistent, and measurable terms.

What is Needed?

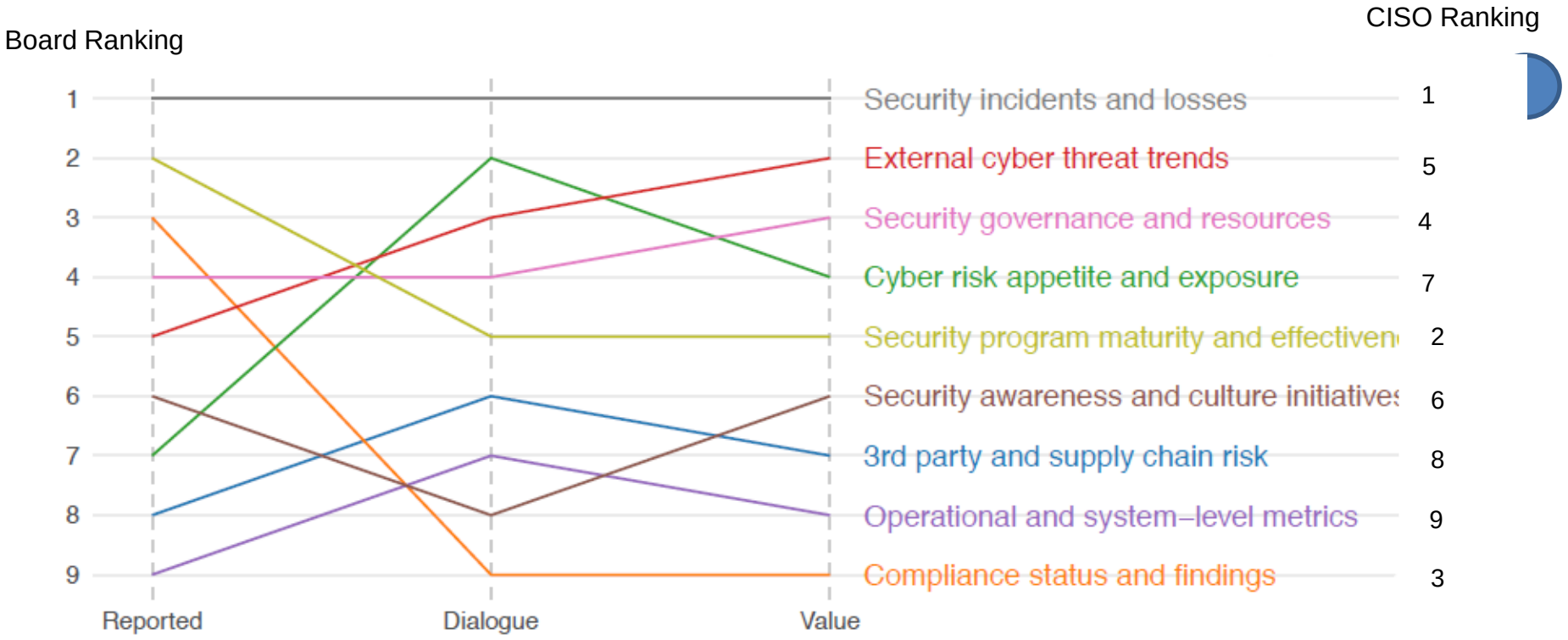


A **shared approach** for discussing the business aspects of cyber risk that meets the needs of all key stakeholders

SERIANU

Cyber Metrics in the Boardroom

Metrics reporting and perceptions



OVERVIEW

OVERVIEW

- The Cyber security problem
- Current State of Cyber security in Organizations
- The Problem with the current state
- The future of Cyber security Management
- The 7 layers of cyber risk exposure management

The Future:
Cyber risk visibility and exposure

Cyber Risk Visibility and Exposure

What is Cyber Risk Visibility?

Cyber risk visibility is the ability to adequately measure the effectiveness and efficiency of implemented cyber security controls to safeguard the organization.

What is Cyber Risk Exposure?

Cyber risk exposure refers to the potential loss an organization faces based on security controls implemented to safeguards its assets

Lack of metrics

- **Financial statements vs Cyber-risk Matrix**

Balance Sheet

As of December 31, 2016 (000s)

What the Company Owns

Assets

Cash	481
Marketable Securities	1,346
Accounts Receivable	1,677
Inventory	2,936
Prepaid Expenses	172
Other Current Assets	58
Total Current Assets	6,670
Gross Value of Property, Plant & Equipment	2,019
Accumulated Depreciation	(664)
Net Property, Plant, Equipment	1,355
Note Receivable	349
Total Assets	**8,374**

What the Company Owes

Liabilities

Accounts Payable	625
Current Portion L-T Debt	1,021
Taxes Payable	36
Accrued Expenses	157
Total Current Liabilities	1,839
Long-term Debt	2,332
Total Liabilities	**4,171**

Shareholders' Equity

Owner's Equity

Common Stock and Paid-in Cap	194
Retained Earnings	4,009
Total Shareholders' Equity	4,203
Total Liabilities and Equity	**8,374**

Paul's Plumbing Co.

STATEMENT OF CASH FLOWS

January - September, 2016

	TOTAL
OPERATING ACTIVITIES	
Net Income	1 2,091.53
Adjustments to reconcile Net Income to Net Cash provided by operations:	
Accounts Receivable	0.00
Inventory Asset	-2,000.00
Accounts Payable	0.00
Bank of America Visa, x7421	300.00
Wells Fargo Credit Card	7,220.20
Total Adjustments to reconcile Net Income to Net Cash provided by operations:	5,520.20
Net cash provided by operating activities	2 $7,611.73
INVESTING ACTIVITIES	
Truck	-10,000.00
Net cash provided by investing activities	3 $ -10,000.00
FINANCING ACTIVITIES	
Loan payable - Truck	10,000.00
Opening Balance Equity	2,255.99
Net cash provided by financing activities	4 $12,255.99
Net cash increase for period	5 $9,867.72
Cash at beginning of period	5,500.00
Cash at end of period	6 $15,367.72

Developing metrics for cyber security

Business Reporting

- What the company OWNS (Assets)
- What the organisation OWES
- Total PROFIT made that year
- How the organisation COMPARES with competitors
- PROJECTIONS in revenue

CURRENT _ IT/Security Reporting

- High VULNERABILITIES
- TOOLS needed by IT department
- AUDIT findings for the year

Developing metrics for cyber security

Business Reporting

- What the company OWNS (Assets)
- What the organisation OWES
- Total PROFIT made that year
- How the organisation COMPARES with competitors
- PROJECTIONS in revenue

IT/Security Reporting

THE RIGHT APPROACH - FUTURE

Visibility – ASSETS

Exposure – LIABILITIES

Profit – GAINED VISIBILITY

Loss – GAINED EXPOSURES

Cash Flow – INCIDENT TRENDING

Current State

Risk

Inherent Risk management

Technology | Processes | People

Controls

Controls management

Risk Management (Anticipate Risks)	Vulnerability Management (Detect Vulnerabilities)
Incident Management (Respond to Incidents)	Threat Management (Contain Threats)

Visibility

Deficiencies

Exposure

visibility management

Asset Controls	User Controls	Incident Controls	Continuity Controls
Asset Inventory	User Access Management	Incident Response	Performance and Availability
Configuration Controls	Privileged Access Management	Fraudulent Transactions	Operational Considerations
Vulnerability Management	Training & Awareness	Monitoring and Analysis	Disaster Recovery
Malware			

INCIDENT REPORTING

Incident Monitoring

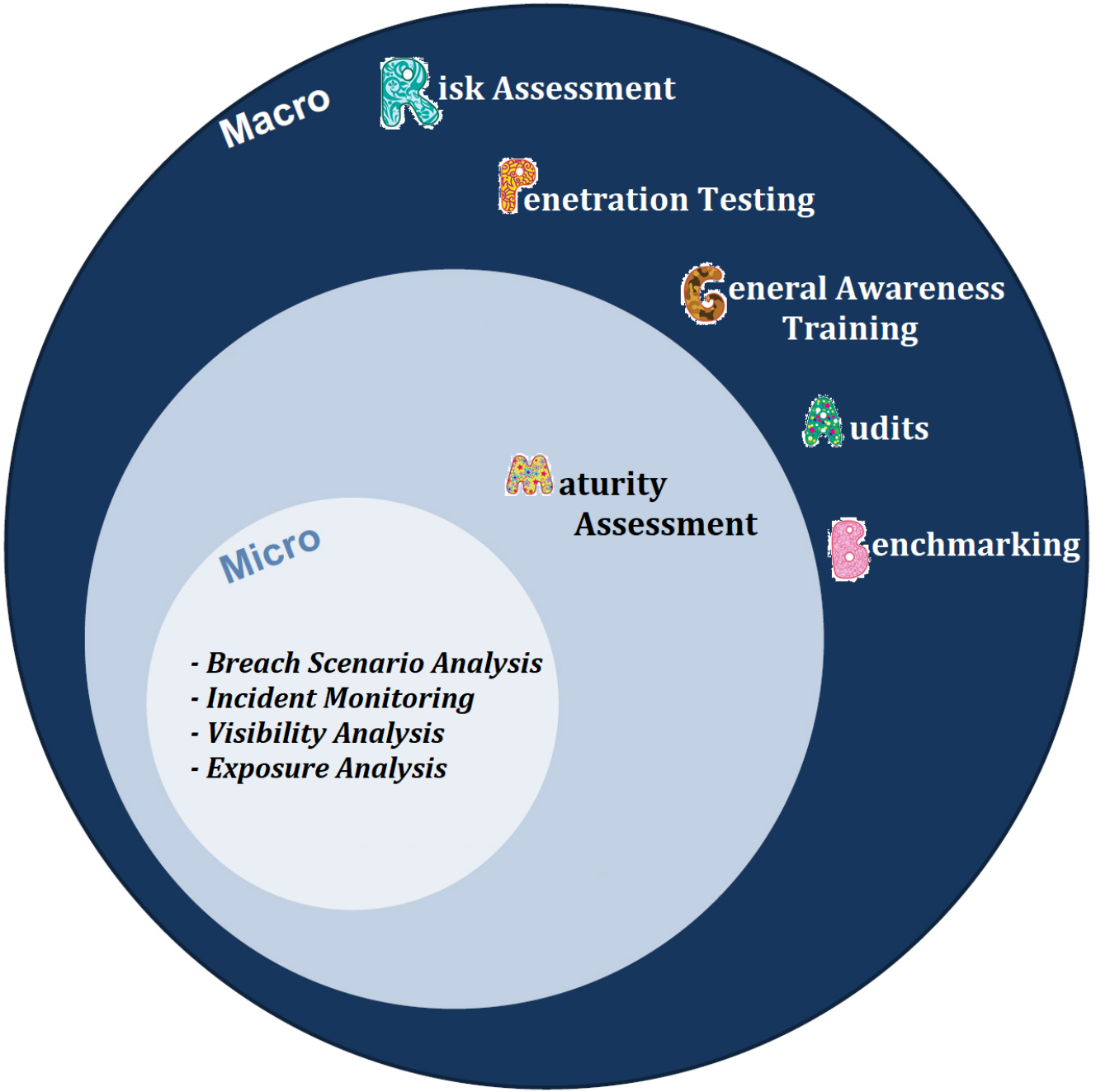
Residual Risk management

Fraud	IP Theft	Sabotage
Email Based Fraud	Data Breach	DDOS
Online Fraud	Hacktivist	Botnet
Wire Transfer	Extortion	Misconfiguration
Mobile Fraud	Domain Theft	Rogue Personnel

Potential Loss

SERIANU

Macro vs Micro Analysis of Risks



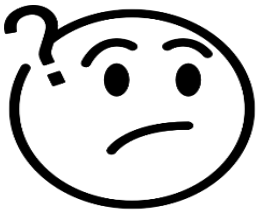
SERIANU

• A new Approach to Cyber security – Continuous Auditing

Regardless of the size, architecture or industry, a security analyst succeeds or fails by their ability to collect and understand:

✓**The right data** at the **right time** in the **right context**.

What should we then focus on?



When it comes down to it, we have two things: **Assets** and **Users.**

SERIANU

- A new Approach to Cyber security – Continuous Auditing

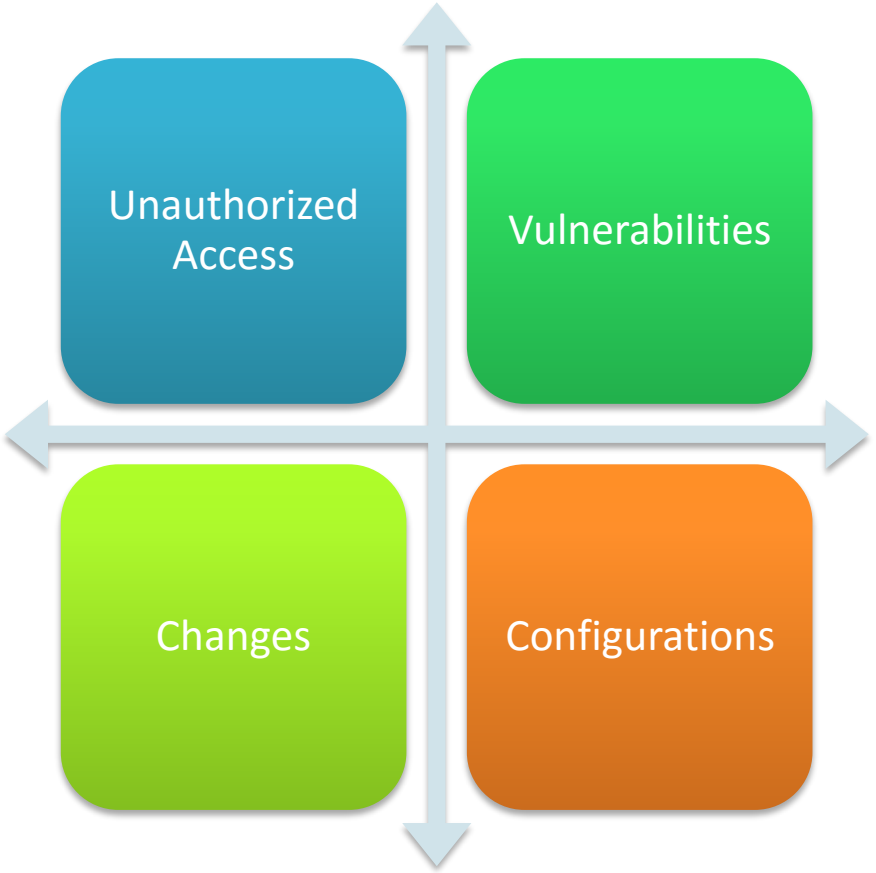
STATIC METRICS

- Vulnerability
- Availability
- Perfomance
- Configuration
- Malware

SERIANU

- A new Approach to Cyber security – Continuous Auditing

Static Metrics



SERIANU

- A new Approach to Cyber security – Continuous Auditing

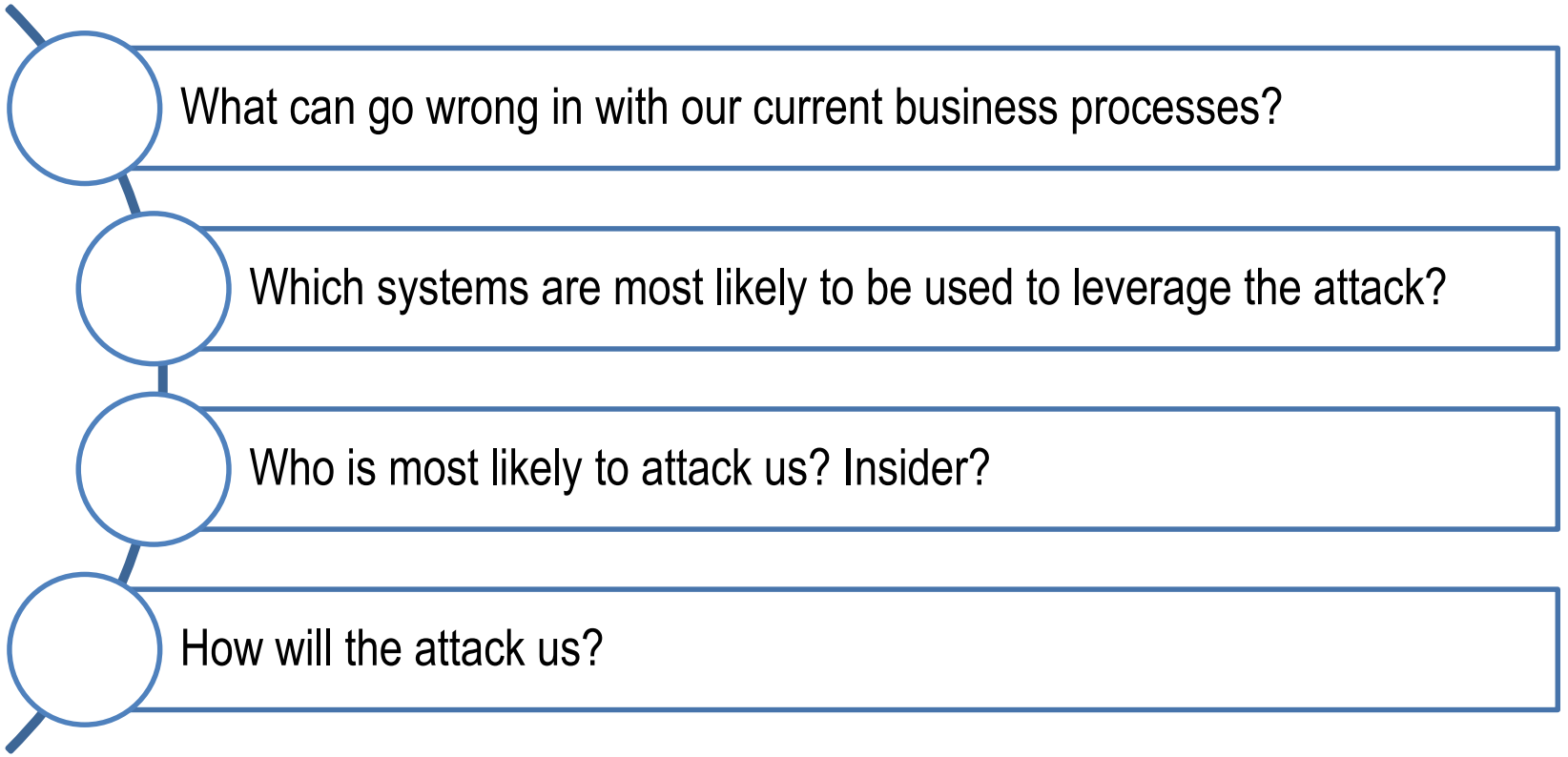
An Analysts key focus should revolve around the following:

- ❑ Threshold Analysis
  - ✓ Volume
  - ✓ Velocity
  - ✓ Limits
  - ✓ Multiplicity
- ❑ Profile Analysis
- ❑ Correlation

SERIANU

• A new Approach to Cyber security auditing – Breach Scenario

Breach Scenario Analysis



OVERVIEW

OVERVIEW

- The Cyber security problem
- Current State of Cyber security in Organizations
- The Problem with the current state
- The future of Cyber security Management
- The 7 layers of cyber risk exposure management

Cyber visibility and exposure management

Current State

Risk

Inherent Risk management

Technology	Processes	People

Controls

Controls management

Risk Management (Anticipate Risks)	Vulnerability Management (Detect Vulnerabilities)
Incident Management (Respond to Incidents)	Threat Management (Contain Threats)

Visibility

Deficiencies

Exposure

visibility management

Asset Controls	User Controls	Incident Controls	Continuity Controls
Asset Inventory	User Access Management	Incident Response	Performance and Availability
Configuration Controls	Privileged Access Management	Fraudulent Transactions	Operational Considerations
Vulnerability Management	Training & Awareness	Monitoring and Analysis	Disaster Recovery
Malware			

INCIDENT REPORTING

Incident Monitoring

Residual Risk management

Fraud	IP Theft	Sabotage
Email Based Fraud	Data Breach	DDOS
Online Fraud	Hacktivist	Botnet
Wire Transfer	Extortion	Misconfiguration
Mobile Fraud	Domain Theft	Rogue Personnel

Potential Loss

Inherent Risk Profiling

- Inherent risk incorporates the type, volume, and complexity of the institution's operations and threats directed at the institution. Inherent risk does not include mitigating controls.

Technology

- External connections
- Wireless connections
- Third parties
- Applications
- Asset inventory
- Channels
- External Threats

Process

- Mergers and Acquisitions
- Change management
- Policies

People

- Staffing
- Training
- Culture

SERIANU

SAMPLE

Inherent Risk Score: 15 **Inherent Risk Posture:** Organization X has significant inherent risk as majority of the controls fall within significant risk.

INHERENT RISK METRICS

Technology

Organization X currently uses Telnet which is an unsecure connection. Guest and corporate wireless networks haven't been segregated within organization X. Organization X therefore has a score of 5.

Processes

Organization X has are in discussions with 1 party for a possible merger. There is high level turnover in the number of network administrators. Organization X therefore has a score of 7.

People

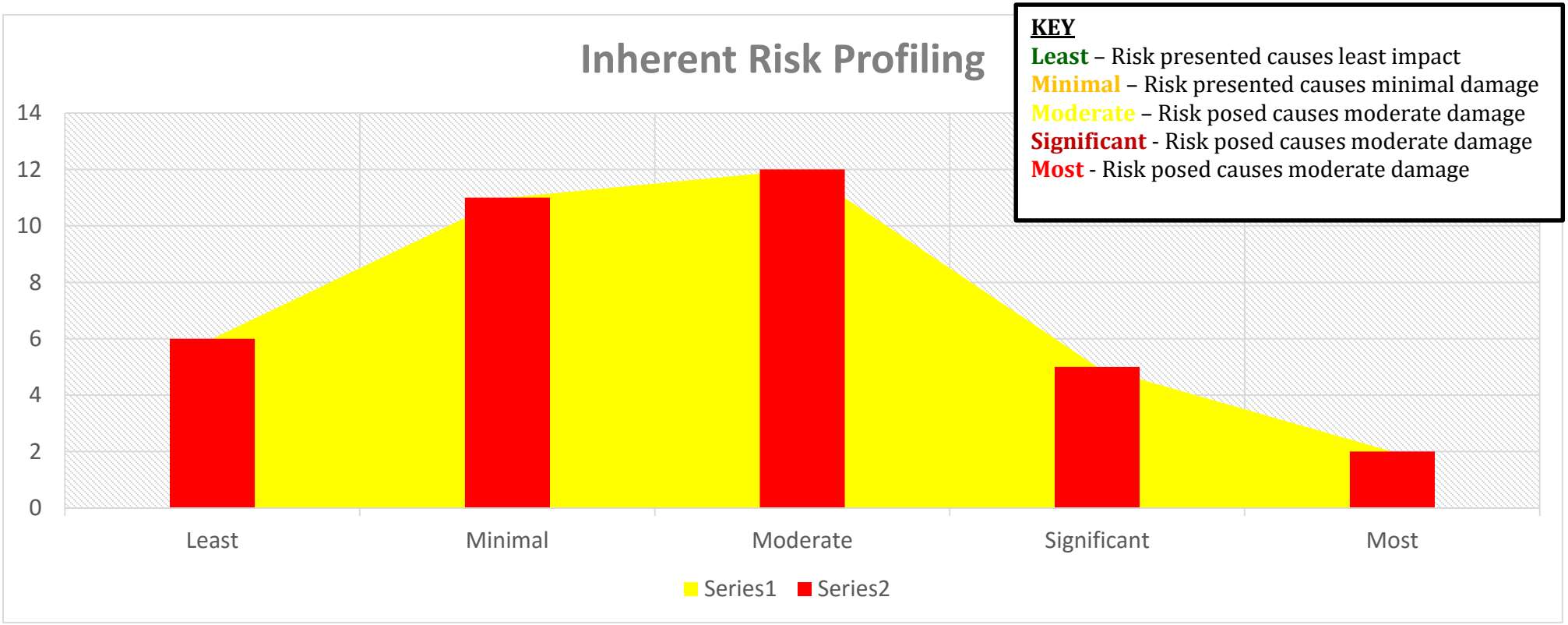
Organization X has no defined information security personnel. There is minimal management involvement in cybersecurity cultural awareness. Organization X therefore has a score of 3.

Domain(s)	Least	Minimal	Moderate	Significant	Most	Total
Domain 1: Technology	0	0	0	3	2	5.00
Domain 2: Processes	0	1	2	3	1	7.00
Domain 3: People	0	1	1	2	1	3.00
Total	0	2	3	8	4	15.00

SERIANU

SAMPLE

Inherent Risk Profiling



KEY

Least – Risk presented causes least impact

Minimal – Risk presented causes minimal damage

Moderate – Risk posed causes moderate damage

Significant - Risk posed causes moderate damage

Most - Risk posed causes moderate damage

Maturity Assessment

- Designed to help management measure the institution's level of risk and corresponding controls. The levels range from baseline to innovative.
  - Anticipate Risk – Cyber Risk management
  - Detect Vulnerabilities – Cyber Vulnerability Management
  - Respond to Incidents – Cyber Incident Management
  - Contain Threats – Cyber Threat Management

Serianu
CVEQ™ Framework

CVEQ™ MATURITY STATEMENT

Report on your organisation's cybersecurity posture.

Wakanda Financial Services Ltd

As at 31st March 2019

Maturity Score: 1.33

Maturity Posture:
The organisation is cyber **Informed.**

CYBER RISK MANAGEMENT

- DOMAIN 1: GOVERNANCE AND STRATEGY
- DOMAIN 2: RISK MANAGEMENT
- DOMAIN 3: PEOPLE AND CULTURE
- DOMAIN 4: INFRASTRUCTURE MANAGEMENT
- DOMAIN 5: ACCESS AND DATA MANAGEMENT
- DOMAIN 6: THIRD PARTY MANAGEMENT
- DOMAIN 7: BUSINESS CONTINUITY MANAGEMENT

CYBER VULNERABILITY MANAGEMENT

- DOMAIN1: VULNERABILITY MANAGEMENT
- DOMAIN 2: PATCH MANAGEMENT
- DOMAIN 3: EXTERNAL DEPENDENCY MONITORING

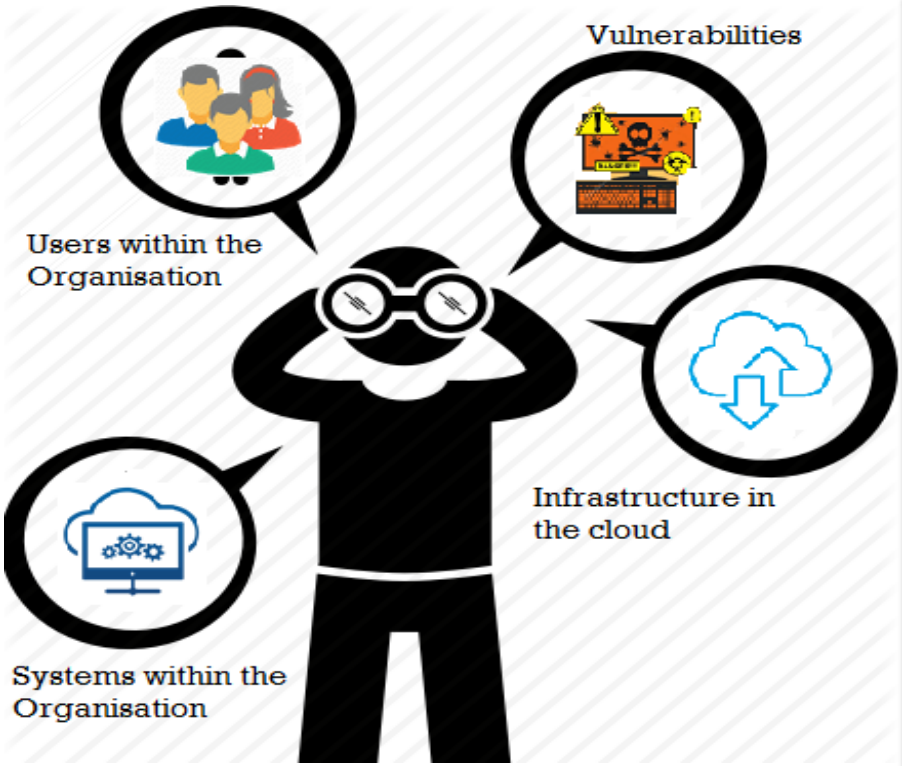
CYBER INCIDENT MANAGEMENT

- DOMAIN 1: EVENT DETECTION
- DOMAIN 2: RESPONSE AND MITIGATION
- DOMAIN 3: THREAT INTELLIGENCE

CYBER THREAT MANAGEMENT

- DOMAIN 1: CYBER RISK REMEDIATION
- DOMAIN 2: INFORMATION SHARING
- DOMAIN 3: METRICS AND REPORTING
- DOMAIN 4: CONTINUOUS IMPROVEMENT

Cyber Visibility Measurement – Balance sheet



The cyber security balance sheet.

Reports the level of visibility that management have into cyber security posture of the organisation

It is based on the cyber security resources, investments and details of a company security posture on a specific day.

This is a snapshot of what the company looked like at a certain time in history.

- Existence and Completeness – Design assertions
- Timeliness and reporting - Operational assertions

SERIANU

The Cyber Visibility and Exposure Statement

The Cyber-Security Balance Sheet as at 31st March 2019

					Overall Visibility	41.4%
Control Areas	**Year**	**Existence**	**Completeness**	**Timeliness**	**Reporting**	**Visibility Score**
Asset Controls						
Asset Inventory, Configuration Controls and Vulnerability Management Malware	Q1 2019	75%	50%	25%	15%	51.5%
	Q4 2018	50%	40%	35%	15%	40.5%
	Q3 2018	40%	30%	25%	20%	32%
User Controls						
User Access Management, Privileged Access Management, Training and Awareness	Q1 2019	75%	70%	55%	45%	66.5%
	Q4 2018	45%	35%	30%	25%	37%
	Q3 2018	50%	40%	35%	30%	42%
Incident Controls						
Incident Response, Fraudulent Transactions, Monitoring and Analysis	Q1 2019	65%	50%	45%	30%	53%
	Q4 2018	55%	40%	35%	35%	44.5%
	Q3 2018	60%	50%	45%	30%	51%
Continuity Controls						
Performance and Availability, Operational Considerations and Disaster Recovery	Q1 2019	60%	53%	50%	40%	53%
	Q4 2018	78%	76%	50%	45%	62.8%
	Q3 2018	40%	35%	35%	20%	35.5%

Legend:

Low Visibility - 0%-25% | **Minimal Visibility** - 26%-50% | **Moderate Visibility** - 51%-75% | **High Visibility** - above 75%

SERIANU

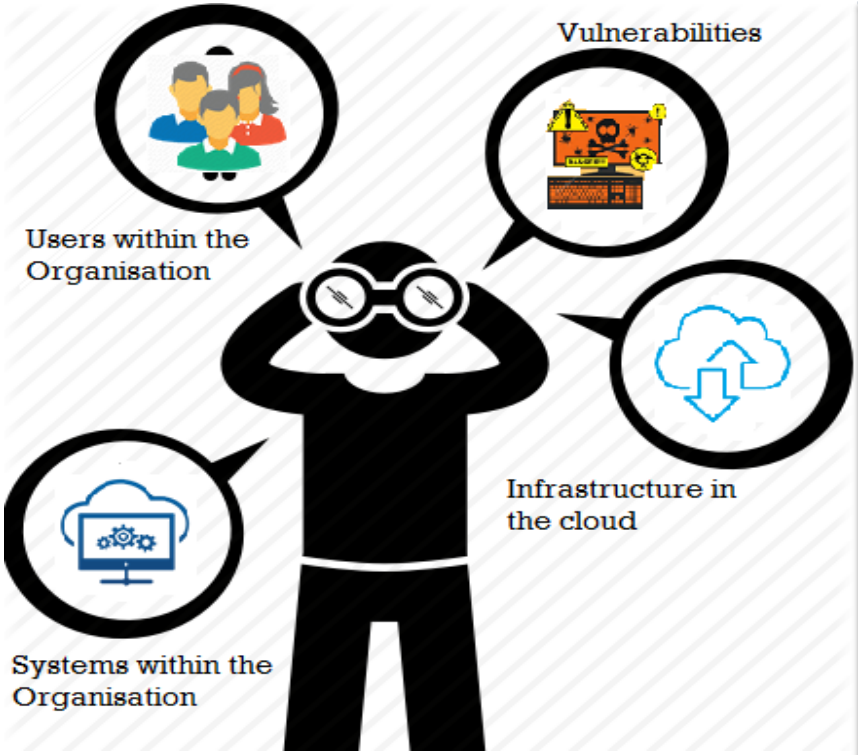
Cyber Exposure (Liabilities)

					Overall Exposure	41.4%
Exposure Areas	Quarter	Asset Controls	User Controls	Incident Controls	Continuity Controls	Exposure Score
Fraud						
Email Based Fraud, Online Fraud, Wire Transfer, Mobile Fraud	Q3 2018	40%	30%	24%	20%	32%
	Q4 2018	50%	40%	35%	15%	41%
	Q1 2019	76%	50%	23%	15%	52%
IP Theft						
Data Breach, Counterfeit, Domain Theft, Unauthorized Disclosure	Q3 2018	49%	40%	35%	30%	42%
	Q4 2018	45%	35%	30%	25%	37%
	Q1 2019	77%	70%	55%	45%	67%
Sabotage						
DDOS, System Outage, Data Hijacking, Data Manipulation	Q1 2019	50%	46%	30%	25%	42%
	Q4 2018	45%	40%	43%	15%	40%
	Q3 2018	45%	35%	30%	25%	37%

Legend:

Low Exposure - 0%-25% | **Minimal Exposure** - 26%-50% | **Moderate Exposure** - 51%-75% | **High Exposure** - above 75%

Cyber security Incident Trending (Income statement)



'the cyber security income statement'

Report incidents, activities, and resulting impact positive or negative of an organisation during a specific time period.

Compares the number of incidents in a certain period over a previous period.

Shows key stakeholders and shareholders how efficiently the company is at mitigating cyber security threats from available resources.

- Design and operations deficiencies
- Significant and material deficiencies

SERIANU

THE CYBER SECURITY DEFICIENCY AND INCIDENT STATEMENT

User Management	Design	Operating	Significant	Material
2018	30	60	58	60
2017	66	56	53	56
2016	56	46	36	46

Privileged Accounts	Design	Operating	Significant	Material
2018	80	75	70	75
2017	77	70	67	70
2016	70	65	60	65

Malware and Viruses	Design	Operating	Significant	Material
2018	56	42	33	42
2017	55	40	30	40
2016	20	32	26	32

Monitoring and Analysis	Design	Operating	Significant	Material
2018	68	63	61	63
2017	63	60	55	60
2016	60	55	51	55

SERIANU

SEC Issues Guidance on Public Company Cybersecurity Disclosure

Freshfields Bruckhaus Deringer LLP



USA | March 15 2018

Gartner Names Risk Quantification a Critical Capability of Integrated Risk Management

by Bryan Smith
June 13, 2018

Share Share Tweet

Are you able to effectively evaluate your cyber security risk in business terms? Last week **Gartner** listed "Risk Quantification & Analytics" as part of five critical capabilities of IRM. If you're not quantifying you're not truly evaluating cyber risk, according to the leading technology analyst firm.

Gartner's Integrated Risk

3.1 Governance

a) Board of Directors

All board members should understand the nature of their institution's business and the cyber threats involved. Robust oversight and engagement on cyber risk matters at the board level promotes a security risk conscious culture within the institution. The responsibilities of the board in relation to cyber risk include:

viii. Review on a regular basis the implementation of the institution's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls. The review should be done at least once in 12 months.
ix. Incorporate cybersecurity as a standard agenda in Board meetings.
x. Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.
xi. Ensure the cybersecurity policy incorporates monitoring metrics coupled with reporting and trend analysis.

William.Makatiani@Serianu.com

https://www.serianu.com