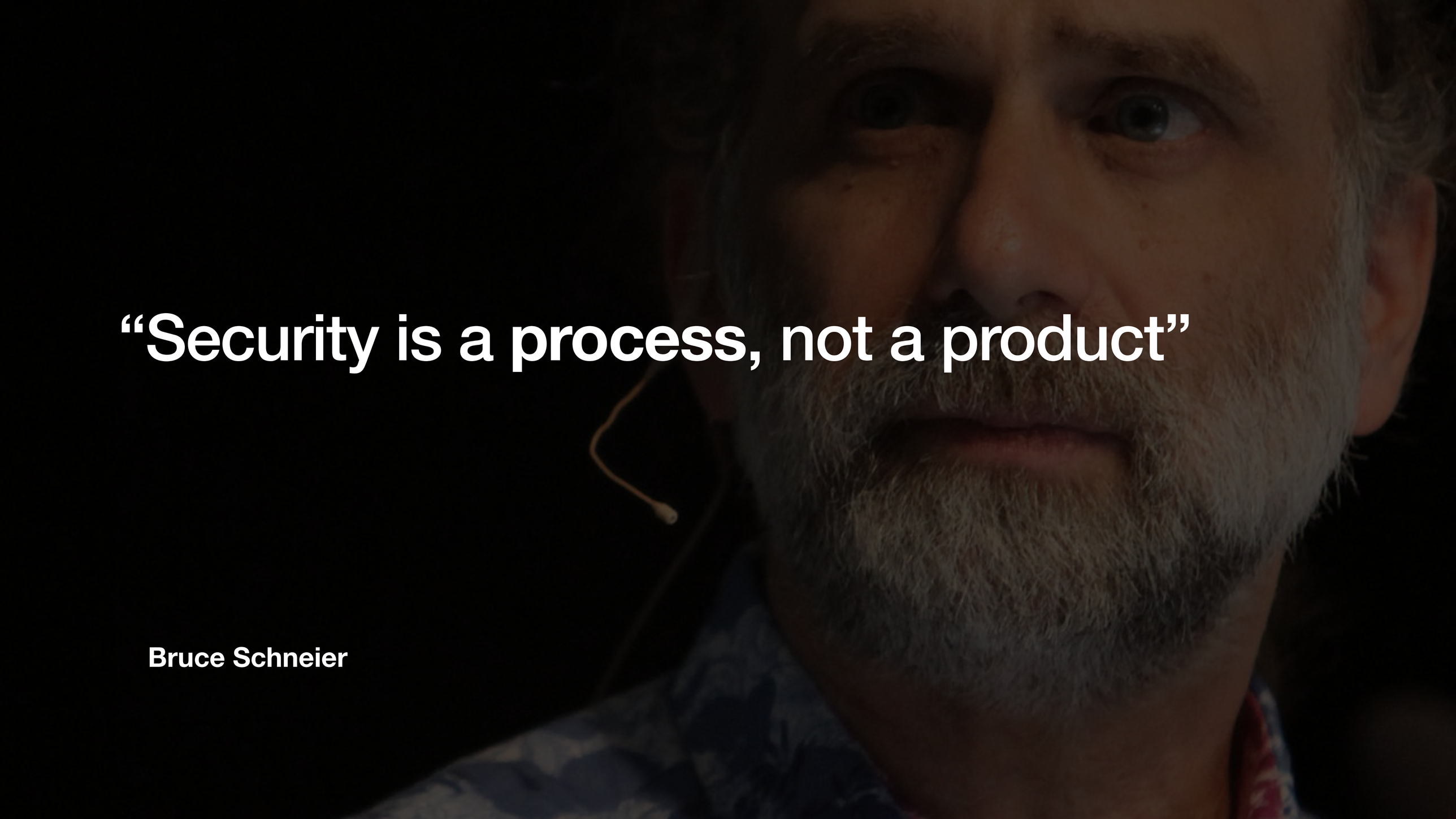
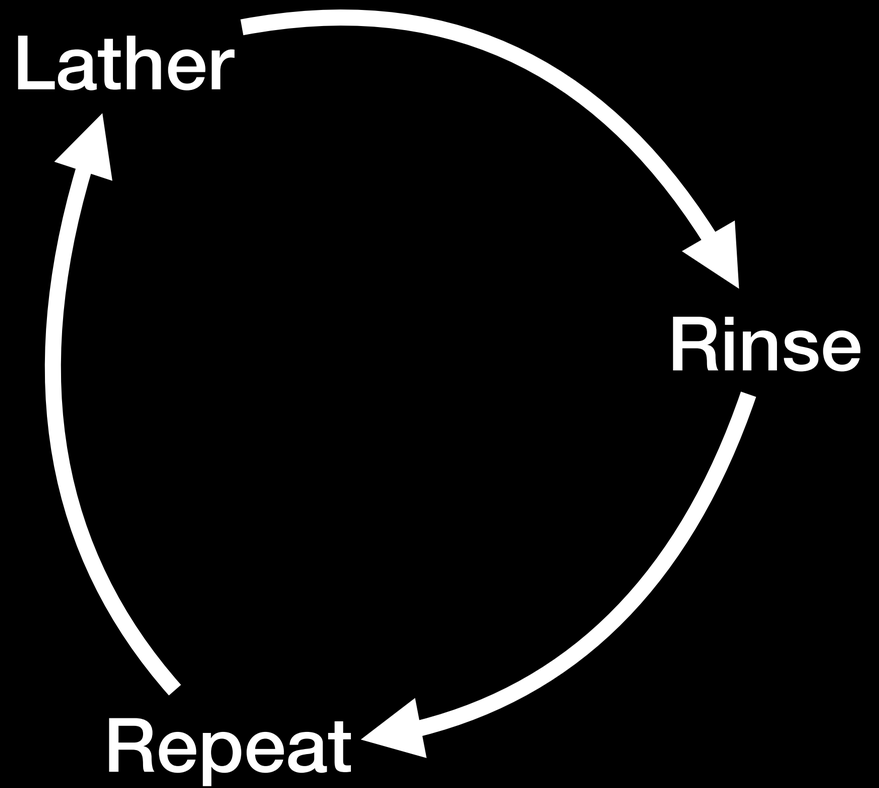
Metrics


“Security is a process, not a product”
Bruce Schneier

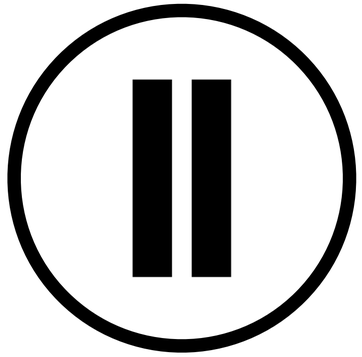
Shampoo algorithm



Quantifying Risk

- **Quantifying** risk is much harder, than identification of risk. Asset understanding must be established and this requires asking difficult questions.
- The **value of the asset** must be understood as well as the **expense of the controls** as well as **cost comparison** with peers.
- **Reaching a consensus** on just a single question can be a challenge.

How do we determine house prices?



Escaping the shampoo algorithm

- Escaping the shampoo algorithm requires individuals to consider if **interventions are working as assumed and working properly**.
- **Key indicators** or metrics can be used to determine if interventions are working as expected.

Key Performance Indicators

Inventory Turnover

COMPANY	TURNS	COMPANY	TURNS
APPLE		COLGATE	
AMAZON		PEPSI	
MCDONALDS		SAMSUNG	
DELL		NIKE	
P&G		INDITEX	
COCA-COLA		STARBUCKS	
INTEL		H&M	
CISCO		NESTLE	
WALMART		RIM	
UNILEVER		CATERPILLAR	

Inventory Turnover

COMPANY	TURNS	COMPANY	TURNS
APPLE	74.1	COLGATE	5.3
AMAZON	10.0	PEPSI	7.7
MCDONALDS	142.4	SAMSUNG	17.1
DELL	35.6	NIKE	4.6
P&G	5.5	INDITEX	4.0
COCA-COLA	5.8	STARBUCKS	6.2
INTEL	5.0	H&M	3.6
CISCO	11.0	NESTLE	4.9
WALMART	8.3	RIM	11.3
UNILEVER	6.0	CATERPILLAR	3.4

Inventory Turnover

- One of many metrics that has the potential to inform **understanding** about holding cost.
- Considering or reducing holding cost has the potential to **improve** overall profits.
- Increased inventory turnover indicates an ability to be **responsive** to changing and a fluid market place as there is smaller amount of obsolete stock.
- Affords **comparison** of performance across competitors, but still difficult to compare across domains.

Inventory Turnover

- Common powerful metrics share common themes:
  - Utilise measurements of time and money.
  - Generated or calculated mechnically and automatically.
  - Understood and communicable across enterprise.
  - Understood across industry and consistently measured.

Metric and Measures

Metric and measures

- Metrics can be considered a measurement of performance, but it is valuable to consider **metrics** and **measures** separately.
  - **Measures** are objective and solid, for example: *% of systems that have been latest software update*.
  - **Metrics** are subjective, at least to some extent, and are focused on how well systems of an organisation are secured.
- Metrics can represent a number of measurements combined.
- Measures and metrics can be employed by enterprises to define **benchmarks**. Benchmarks can be used by organisation to improve systems.

Metric and measures

- Metrics and measures can be used by enterprises to:
  - verify compliance of elements inline with policy, standards and procedure
  - determine the strengths and weaknesses of security within the organisation
  - understand performance inline with peers and general trends.

Metric and measures

- Metrics and measures can be used by management:
  - improve performance of controls and policy
  - answering important questions at the management level
  - evaluation of policy in line compliance and legislation.

Motivation for Metrics

Motivation for Metrics

- Often the aim is to remove **fear**, **uncertainty** and **doubt** (FUD) with strong security measurements.
- **Accountability** in terms of demonstrating regulatory compliance.
- **Provable security** in terms of better understanding the money spent on security improvements.
- **Cost** of defence and security improvements are needed to attain funding.

Motivation for Metrics

- Technical perspective metrics can be thought of a standard or system for measurement.
- Metrics can be considered in terms of **process improvement** and **value**.
- Aim of metrics is develop answers and **insight** into the system as a whole.
- Consequently, the best measurements, answers the question, the challenge is determining the **correct question**.

Motivation for Metrics

Security improved this year?

How do I compare to others?

What do I get for security spending?

Business drivers for Security Measurements

Business drivers for Security Measurements

Information asset fragility

Provable security

Cost pressures

Accountability

Information asset fragility

Business drivers for Security Measurements

- Enterprises are complex and large, typically heavily reliant on information and when that information is destroyed or leaked, it causes concerns for management.

Provable security

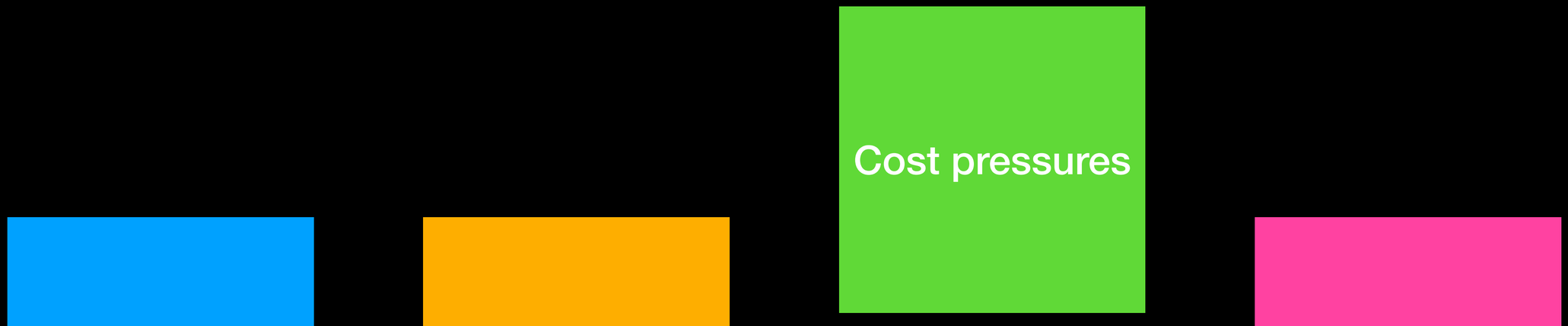
Business drivers for Security Measurements

- Lack of metric and measurements makes it difficult to determine the effectiveness of controls and policy.
- Consequently, organisations become trapped in the shampoo algorithm but never get clean, companies are spending significant amounts of money with little to show for it.

Cost pressures

Business drivers for Security Measurements

- Budgets for security are not infinite, budget holders for security will be competing with other projects within the enterprise.
- Expensive security solutions with no real ability to demonstrate effectiveness are unlikely to secure funds within an organisation.



Accountability

Business drivers for Security Measurements

- Metrics and measurements are valuable in promoting accountability for failures or achievements in cyber security.
- Consider the speedometer, difficult for the driver to state they are not speeding when the speedometer clearly confirms the speed of the vehicle in relation to the context, i.e. speed limit for the road.

Business drivers for Security Measurements

Information asset fragility

Provable security

Cost pressures

Accountability

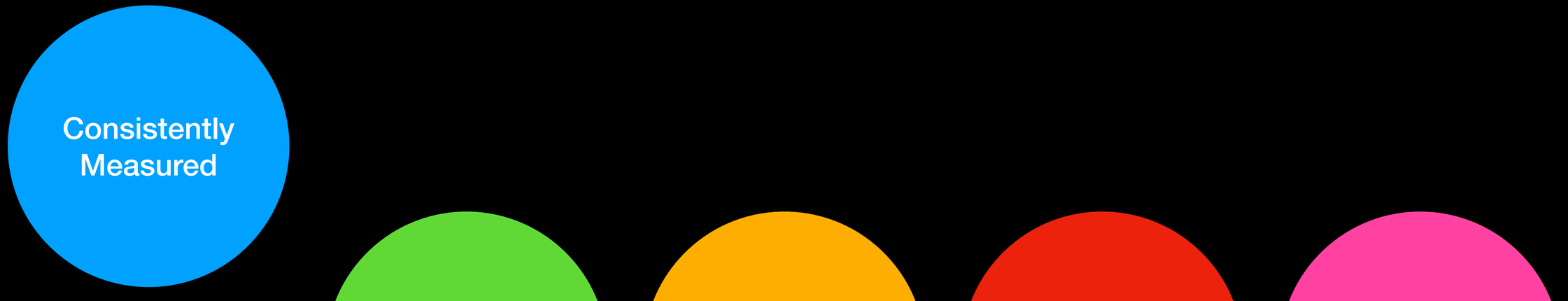
Characteristics of Good Metrics

Characteristics of Good Metrics

Consistently measured

Characteristics of Good Metrics

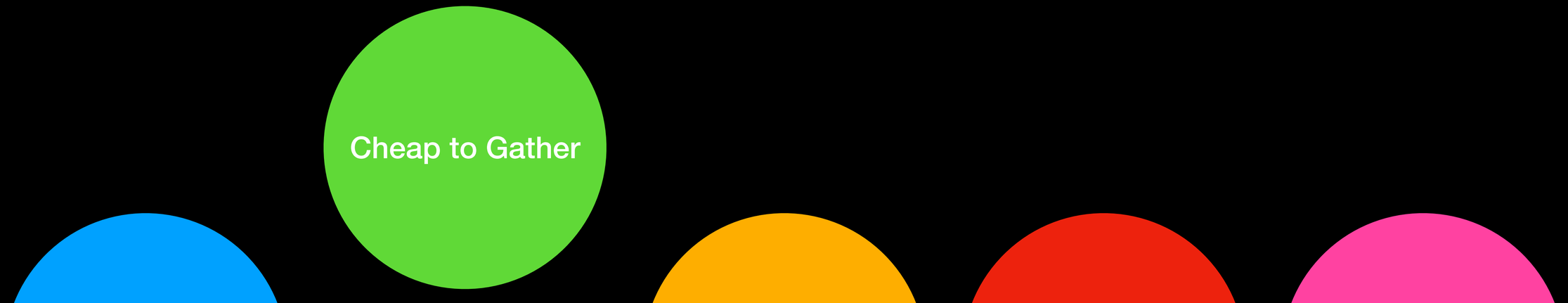
- Metrics that are consistently measured are more credible than those that are not. Individuals and teams should be able to take measurements from the same data or the same element and produce the same answer.
- If the metric is soft, relying on humans and judgement, then it is likely if you ask two different individuals you will get different ratings or judgements.
- Metrics may not be taken directly from elements or data, may be derived.

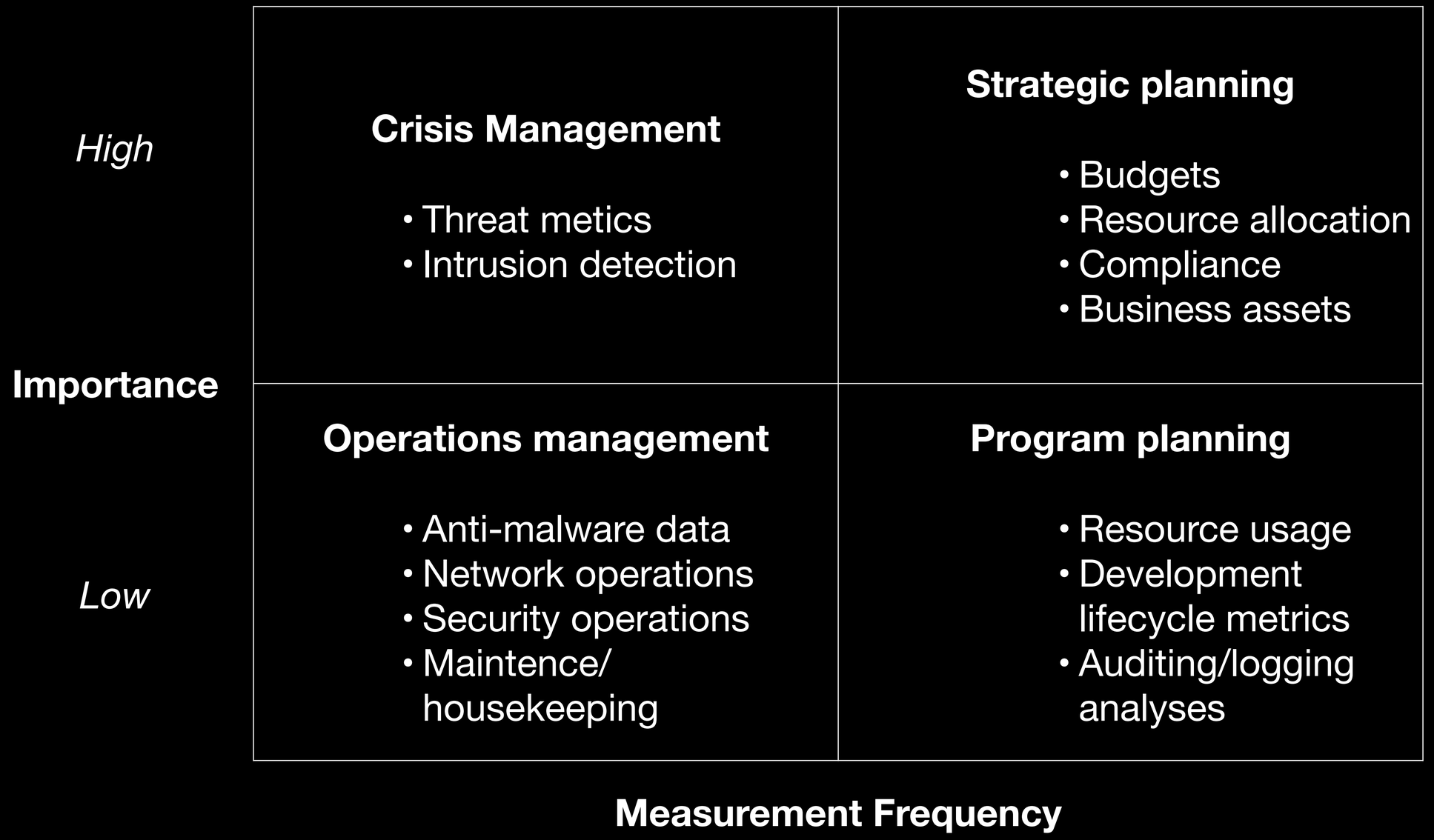


Cheap to gather

Characteristics of Good Metrics

- Metrics can be complex and take time to collect and generate, but the speed at which a metric can be generated and the expense it takes to collect will influence its use.
- Automated metrics will be generated and collected far more, than slower, more ‘manual’ metrics. Faster to collect, more likely it is to inform.



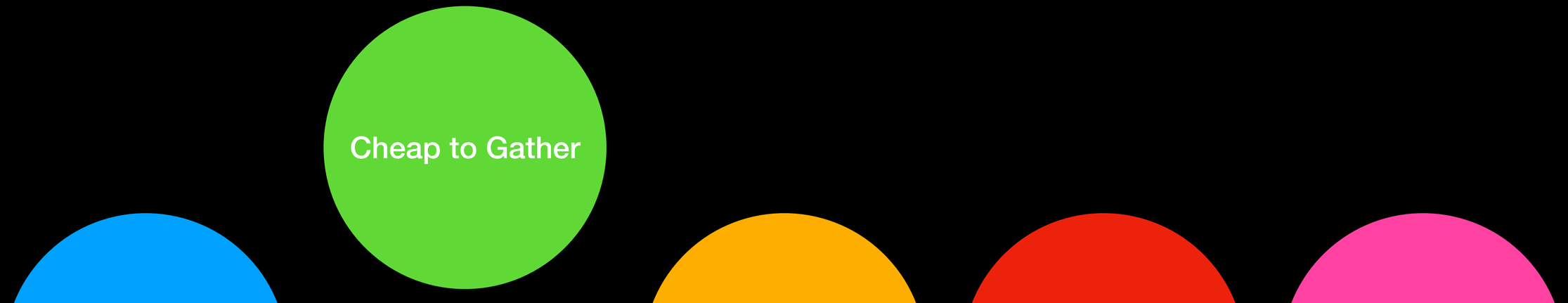


Jaquith, 2007
Security Metrics

Cheap to gather

Characteristics of Good Metrics

- Metrics can be complex and take time to collect and generate, but the speed at which a metric can be generated and the expense it takes to collect will influence its use.
- Automated metrics will be generated and collected far more, than slower, more ‘manual’ metrics. Faster to collect, more likely it is to inform.



Expressed as a number

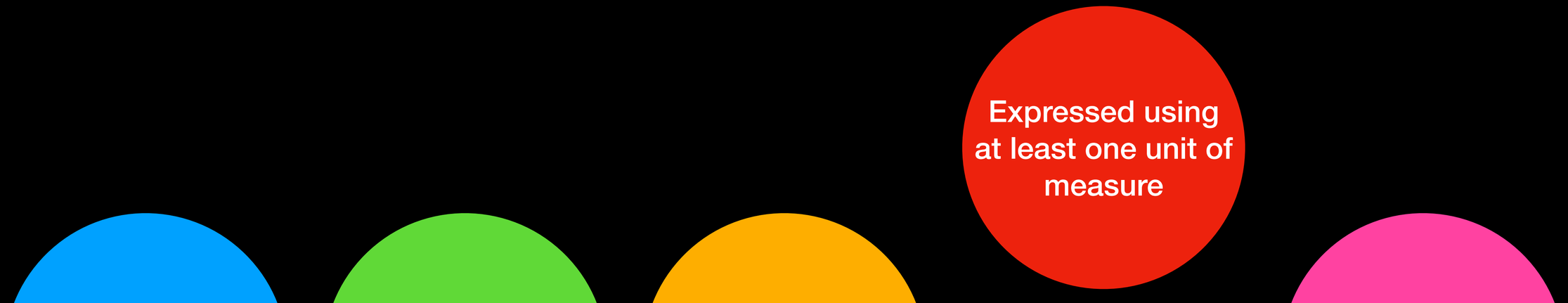
Characteristics of Good Metrics

- Metrics should be expressed as a percentage or number, cardinal in nature rather than ordinal.
- Counts are more valuable than ratings or order, for example: *a traffic light rating is not a good metric.*

Expressed using at least one unit of measure

Characteristics of Good Metrics

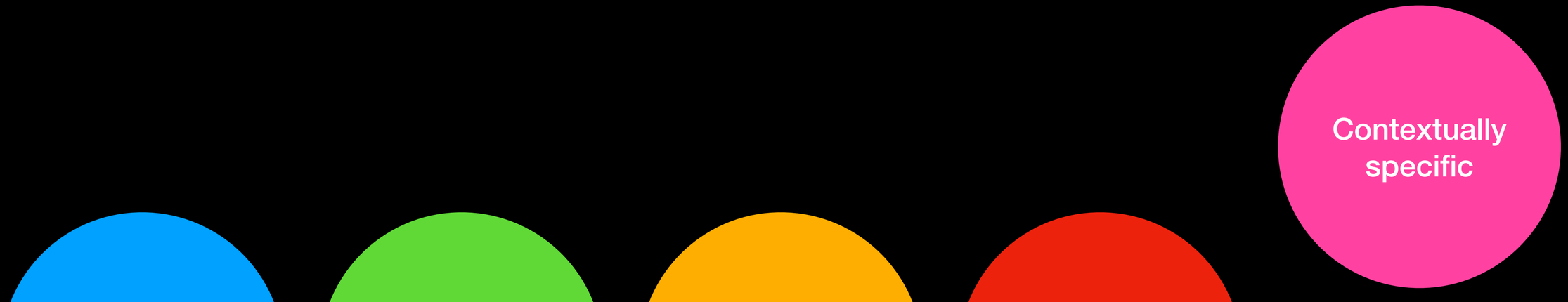
- Metrics that are expressed as a number are strong, but can be strengthened with at least a unit of measurement, for example: *number of malicious emails*.
- Additional units or dimensions of measurements can be added to the metric, for example: *number of malicious emails per 1,000 emails*.



Contextually specific

Characteristics of Good Metrics

- A strong metric is able to communicate information almost immediately, whereas generic metrics may be of little benefit to many.
- Metrics that are tailored to context are far more valuable, for example: *% of malicious emails versus % malicious emails for human resources*.



Characteristics of Good Metrics

Characteristics of Bad Metrics

Characteristics of Bad Metrics

Inconsistently measured

Characteristics of Bad Metrics

- Metrics that are soft, that rely on judgement, or are inconsistently measured are generally consider poor metrics.
- Even metrics that rely on human judgement, if they are to be of any use, must be carefully elicited.

Cannot be gathered cheaply

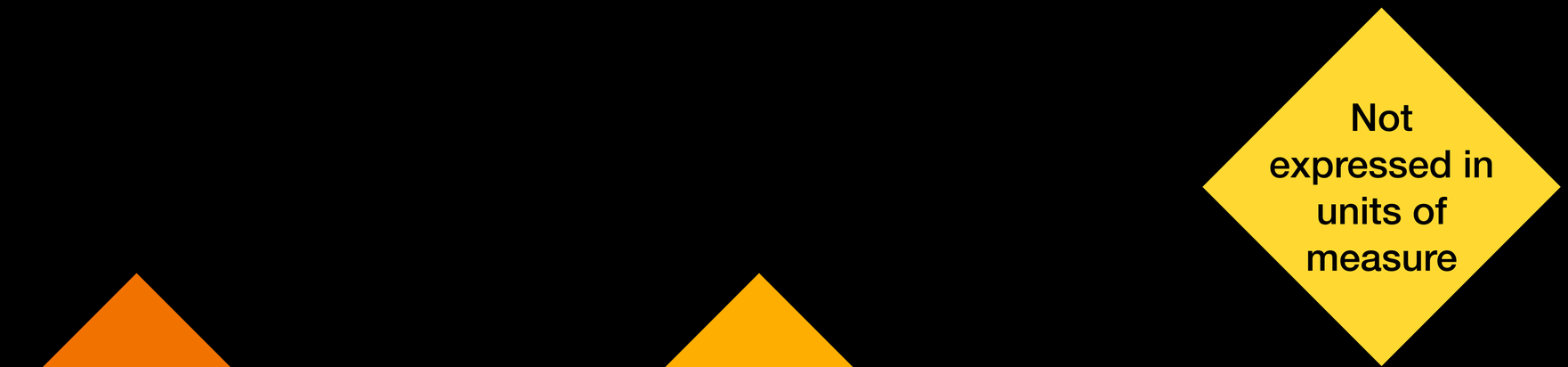
Characteristics of Bad Metrics

- Metrics that can not be collected and generated relatively rapidly are not good metrics as they will inevitably not be collected often.
- Complex and slow metrics may also suffer from poor production as they take time to produce from infrastructure and other controls.

Not expressed in units of measure

Characteristics of Bad Metrics

- Metrics that are ordinal in nature involving ratings and judgements are generally considered poor metrics.



Characteristics of Bad Metrics

What are not metrics?

What are not metrics?

- The aim of metrics is to support the organisation in improving their cyber security, poor metrics do not support this aim.
- Catalogues of metrics, taxonomies and frameworks can provide libraries of metrics, but these more often than not may not be useful.
    - Libraries of metrics can be valuable in inspiring individuals to determine the best metrics for their organisation, but generally should be selected and insert without thought to context.

Audience

Audience

- Enterprises should rely on a number of metrics, spread across levels and hierarchies.
- Management will want metrics that support them in answering high-level questions, for example: *how does the organisation's security cost contrast to peers?*
- Technical teams will want metrics at the lower-level that advise the performance of specific technical controls or concerns, for example: % *malicious code detected in stored files.*

What are the best Metrics to select?

What are the best Metrics to select?

- The best metrics for the organisation are those metrics and measurements that answer valuable question.
- The **important starting point is the question the organisation wants to answer** and then from that question, organisations should determine the metrics and measurements that allow them to answer it.

Problems with Metrics and Measures

Problems with Metrics

Accuracy

- Even with perceived strong metrics there can be a **level of imprecision** that can impact on the organisation. For example: patch management may communicate at the operating system-level, application-level etc.
- **Clarity around measurement methods** and procedures to collect measurements and generate metrics. For example: some organisations may rely on third-party measurements or systems where it is not clear how the measurement has been collected.
- Many metrics within an organisation can be **used without sufficient context**, making it difficult to appreciate the value of the metric and/or measurement in a given context.
- **Fluid use of language** in cyber security and computing could result in poor interpretation or understanding of metrics and measurements.

Problems with Metrics

Selection

- Organisations may favour measurements and metrics that are cheap and easy to collect without understanding the value of them. The concern with this approach:
  - Organisations waste time and resource collecting meaningless data.
  - Generate misleading results, if there is not a clear understanding in how the measurements relate to each other.
  - Individuals that collect measurements, that perceive them as useless may become disgruntled or have concerns about the security of the organisation.
- Concerns with metrics and measurements that are collected by humans is that they may favour metrics that are easy to collect or demonstrate positive posture.

Problems with Measures

- Metrics can represent the combination of measures, but it is important that individuals to generating metrics understand how to properly combine measurements - if not the metric will be at best useless at worse misleading.
- Organisations will continue on a process to improve cyber security, metrics that seemed reasonable in early cycles, may be problematic or pointless in later cycles. Consequently, organisations will want to revise and review metrics over time.


Sample Copy
Clear/Stop
Start
Enter

Examples of Metrics

Email

Examples of Metrics

METRIC	MOTIVE	SOURCE
ENCRYPTED MESSAGES PER DAY (%, COUNT)	UNDERSTANDING LEVEL OF ENCRYPTED TRAFFIC	EMAIL SYSTEM
SPAM FN (%, COUNT)	ACCURACY OF SPAM DEFENCES	GATEWAY DEFENCE SOLUTION
SPAM FP (%, COUNT)	ACCURACY OF SPAM DEFENCES	GATEWAY DEFENCE SOLUTION
TYPICAL ATTACHMENT SIZE	UNDERSTANDING EMAIL TRAFFIC PER BLOCK	EMAIL SYSTEM
VIRUS TP (%, COUNT)	ACCURACY OF VIRUS DEFENCES	GATEWAY DEFENCE SOLUTION
TYPICAL EMAIL SIZE	UNDERSTANDING EMAIL TRAFFIC PER BLOCK	EMAIL SYSTEM

Viruses

Examples of Metrics

METRIC	FOCUS	SOURCE
DETECTED SPYWARE ACROSS ALL SYSTEMS (% COUNT)	UNDERSTANDING TYPICAL INFECTION RATES	GATEWAY DEFENCE SOLUTION AND RECORDS
DETECTED VIRUSES FROM WEBSITE (COUNT)	UNDERSTANDING STAFF BEHAVIOUR	GATEWAY DEFENCE SOLUTION
DETECTED SPYWARE FOR SPECIFIC BUSINESS UNITS (COUNT)	UNDERSTANDING TYPICAL INFECTION RATES	GATEWAY DEFENCE SOLUTION
INCIDENTS FROM QUARANTINED FILES (%, COUNT)	UNDERSTANDING STAFF BEHAVIOURS	INTERNAL SUPPORT RECORDS
MANUAL CLEAN UP COST (COST)	ASSOCIATED STAFF COST	INTERNAL TIME AND MOTION DATA
OUTBOUND VIRUS DETECTED (COUNT)	UNDERSTANDING INTERNAL INFECTIONS	GATEWAY DEFENCE SOLUTION

System Configuration

Examples of Metrics

METRIC	FOCUS	SOURCE
HOST BENCHMARK SCORE	INSIGHT INTO CONFIGURATION OF SYSTEMS	BENCHMARKING TOOLS
NUMBER OF REMOTE MANAGED SYSTEMS (COUNT)	REMOTE SYSTEMS THAT MAY REQUIRE SPECIFIC DEFENCE SOFTWARE	SYSTEM MANAGEMENT SOFTWARE, DEFENCE SOFTWARE
EMERGENCY CONFIG. RESPONSE TIME (TIME)	INSIGHT INTO TIME TO RECONFIGURE	TIME TRACKING LOGS
DEFAULT BUILD IMAGE (%)	INSIGHT INTO CONFORMANCE ACROSS	WORKSTATION MANAGEMENT SOFTWARE
MONITORED CRITICAL SYSTEMS (%)	INSIGHT INTO UPTIME AND MONITORING COVERAGE	SYSTEM MANAGEMENT SOFTWARE AND LOGGING
SYSTEMS BEING LOGGED (%, SYSTEM COUNT)	INSIGHT INTO UPTIME AND MONITORING COVERAGE	SYSTEM MANAGEMENT SOFTWARE AND LOGGING

Patch Management

Examples of Metrics

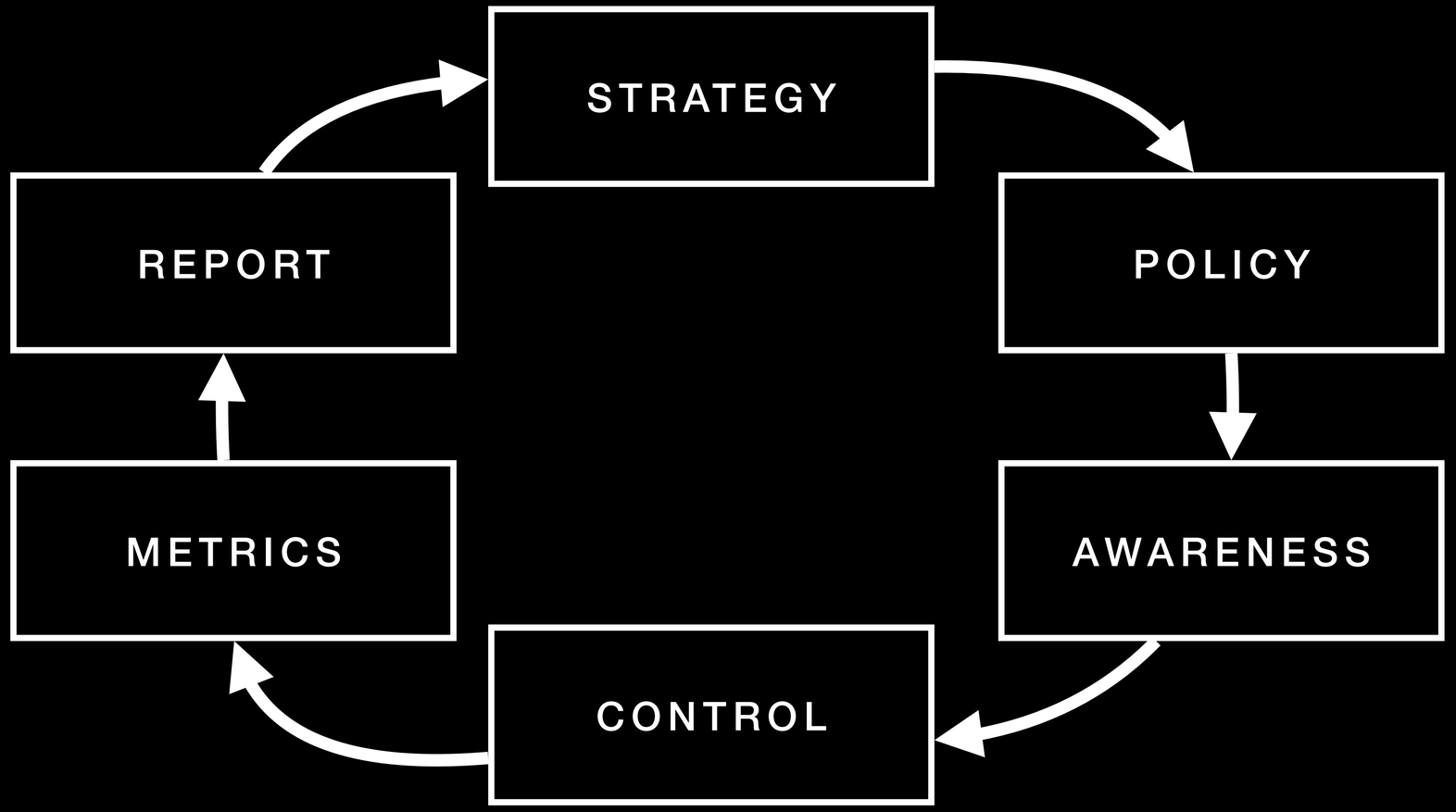
METRIC	FOCUS	SOURCE
NUMBER OF UNAPPLIED PATCHES	INDICATOR OF UNAPPLIED WORKLOAD	PATCH MANAGEMENT SOFTWARE
PATCH EXPENSE FOR SPECIFIC VULNERABILITY	UNDERSTANDING OF EXPENSE	TIME AND MOTION, PATCH MANAGEMENT SOFTWARE
PATCH TEST CYCLE	EXPOSURE TIME BETWEEN RELEASE AND TEST	PATCH MANAGEMENT SOFTWARE
PATCH SLA ACHIEVEMENT	UNDERSTANDING ACHIEVEMENT OF SLA	TIME AND MOTION, PATCH MANAGEMENT SOFTWARE
UNAPPLIED RATIO FOR SYSTEM TYPE	INDICATOR OF PATCH WORKLOAD PER SYSTEM	PATCH MANAGEMENT SOFTWARE
SYSTEMS NOT INLINE WITH PATCH POLICY	UNDERSTANDING REACH OF PATCH MANAGEMENT	PATCH, VULNERABILITY MANAGEMENT SOFTWARE

Uptime

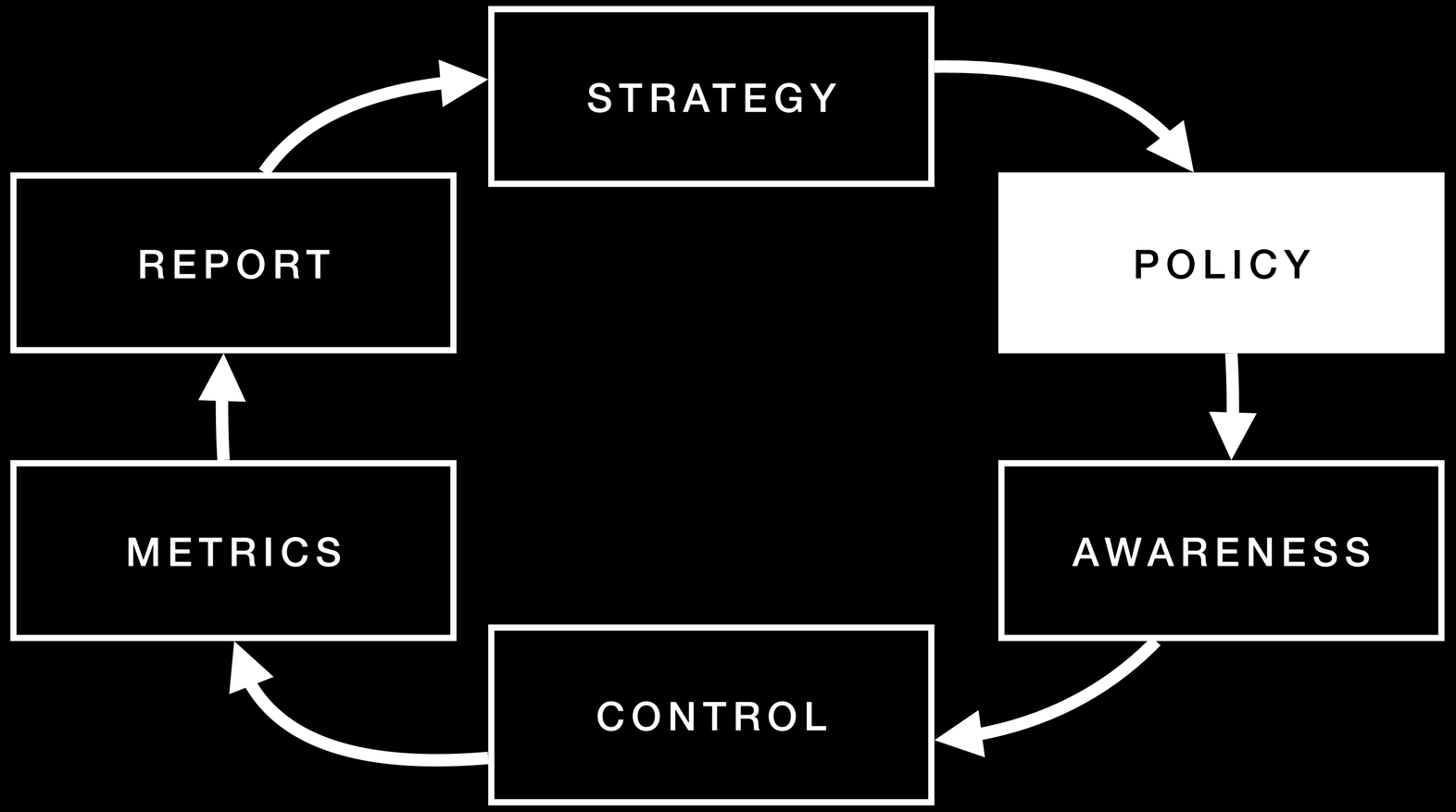
Examples of Metrics

METRIC	MOTIVE	SOURCE
HOST UPTIME (%, TIME)	AVAILABILITY MEASURES FOR CRITICAL HOSTS	LOGS, BOOK KEEPING
UNPLANNED DOWNTIME (%, TIME)	CONTROL INSIGHT AS LARGE NUMBERS WOULD INDICATE POOR CONTROL	BOOK KEEPING
UNPLANNED DOWNTIME DUE TO SECURITY CONCERNS (%, TIME)	CONTROL INSIGHT IN TERMS OF SECURITY	BOOK KEEPING
SYSTEM REVENUE (£, TIME)	BUSINESS VALUE	SPREADSHEETS AND BOOK KEEPING

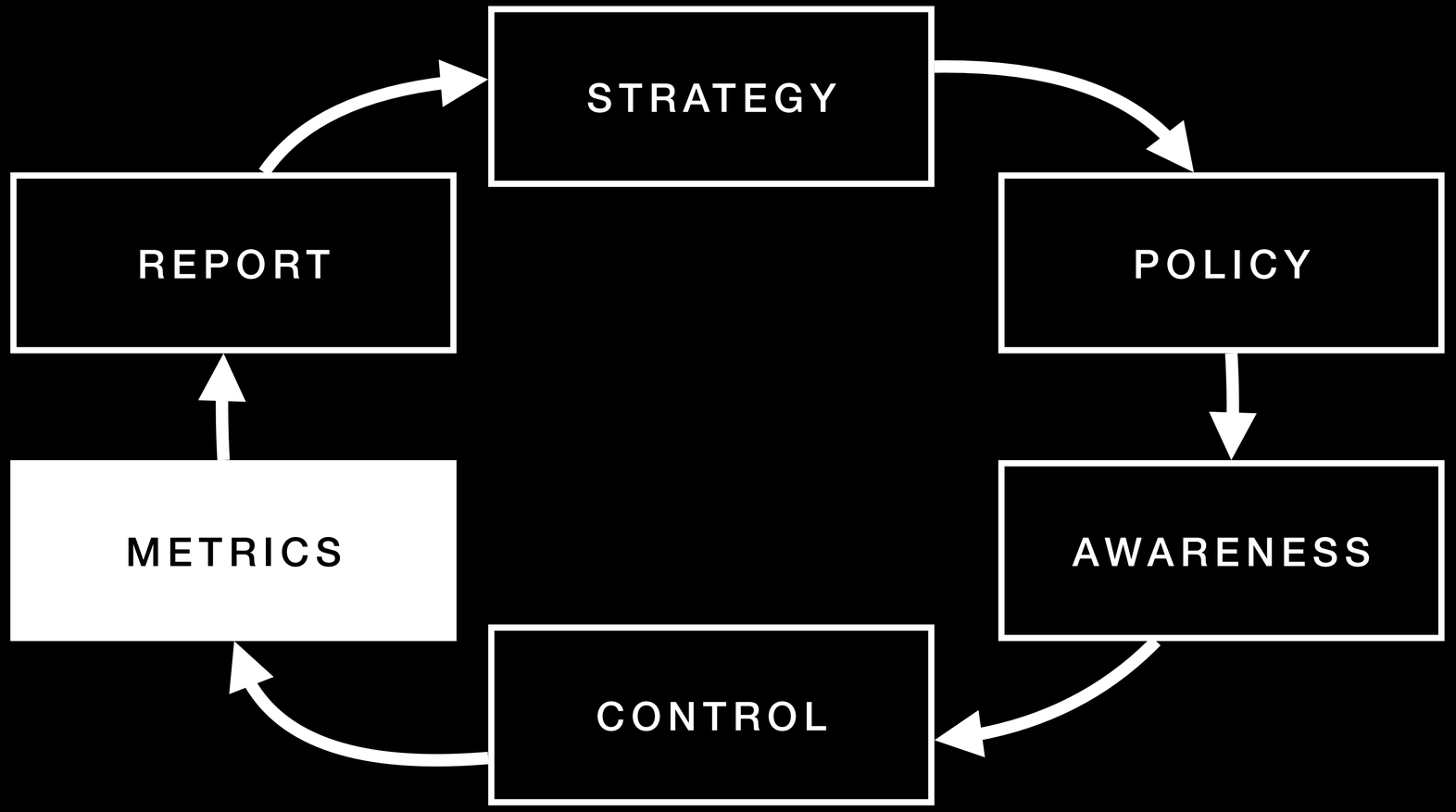
Policy implementation



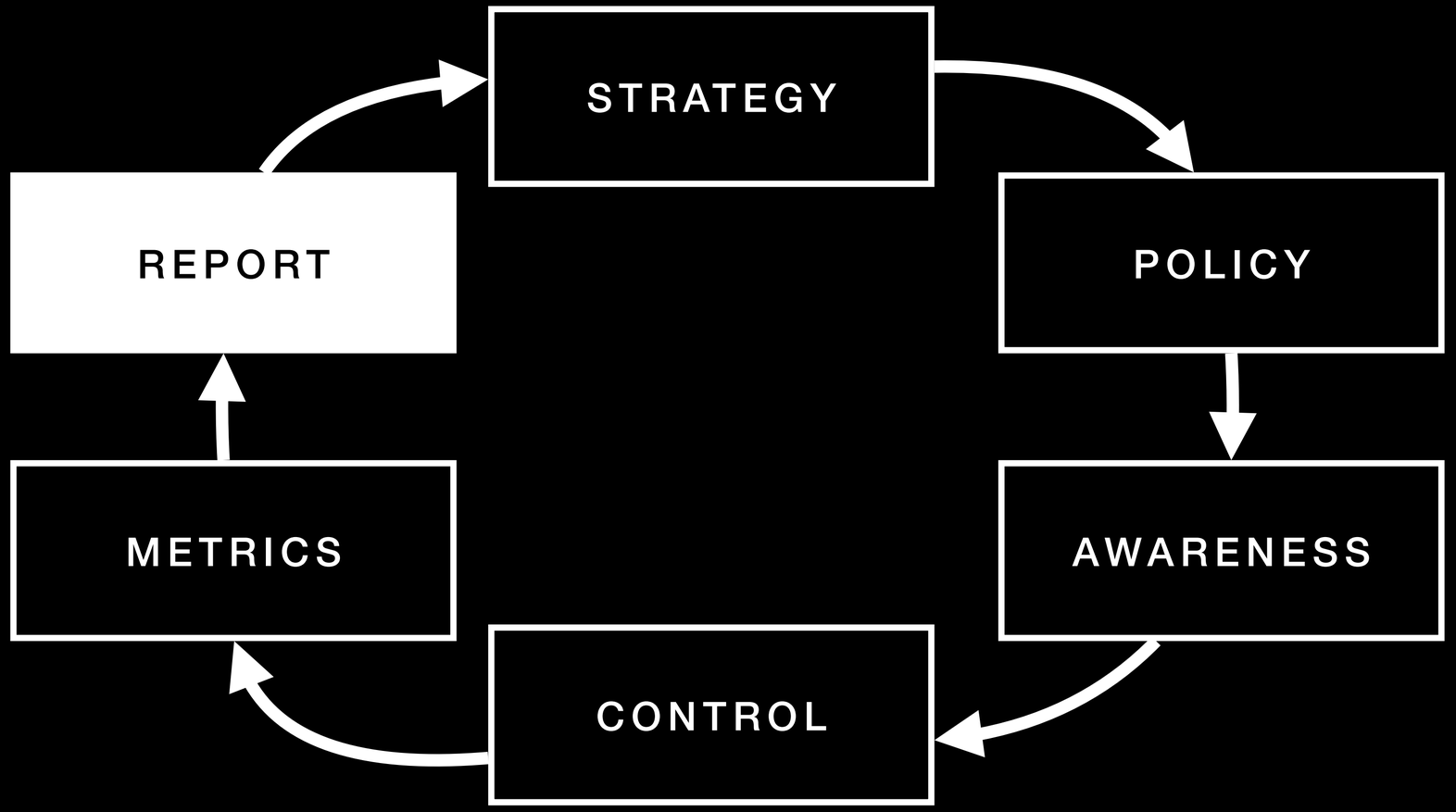
Bayuk, 2007
Cyber Security Management Cycle



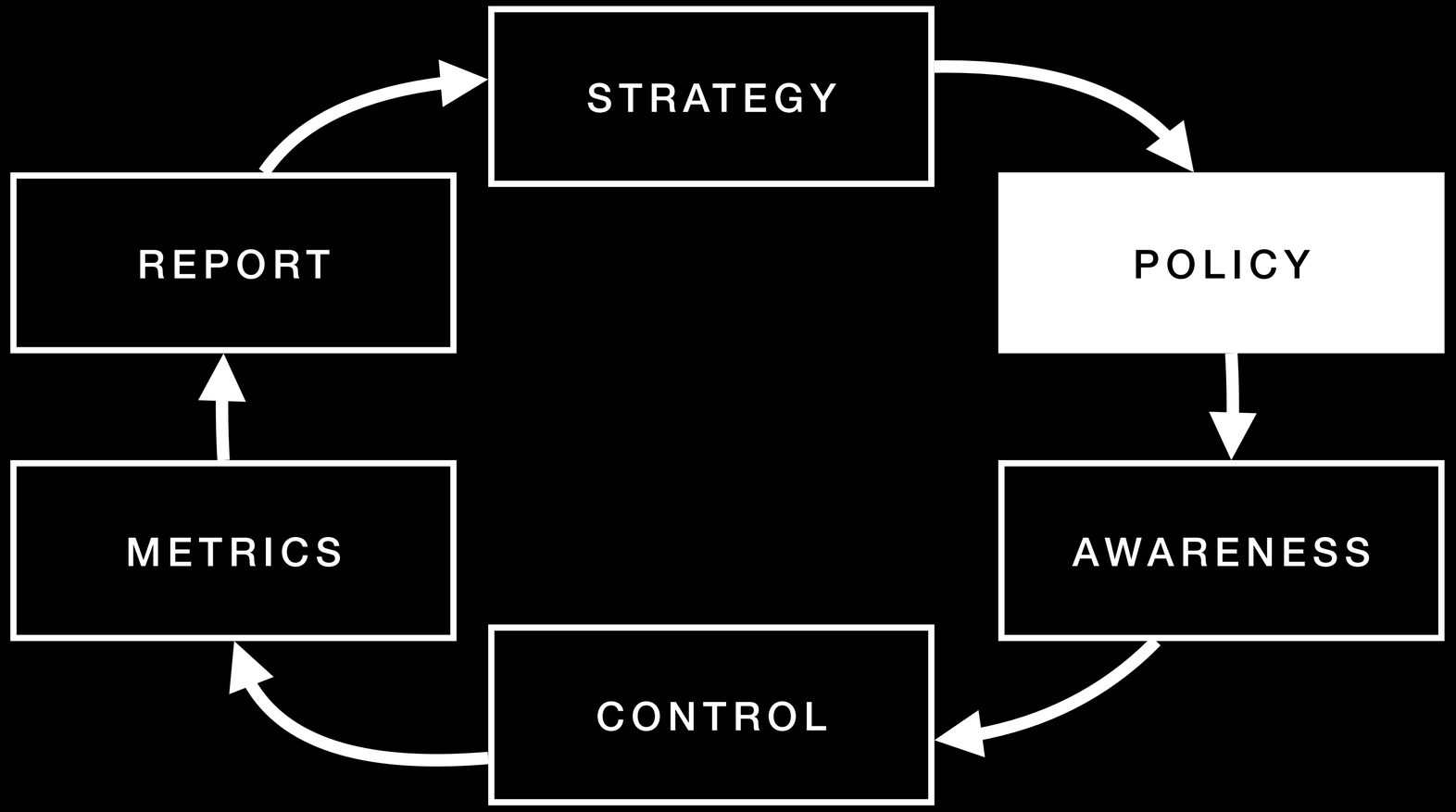
Bayuk, 2007
Cyber Security Management Cycle



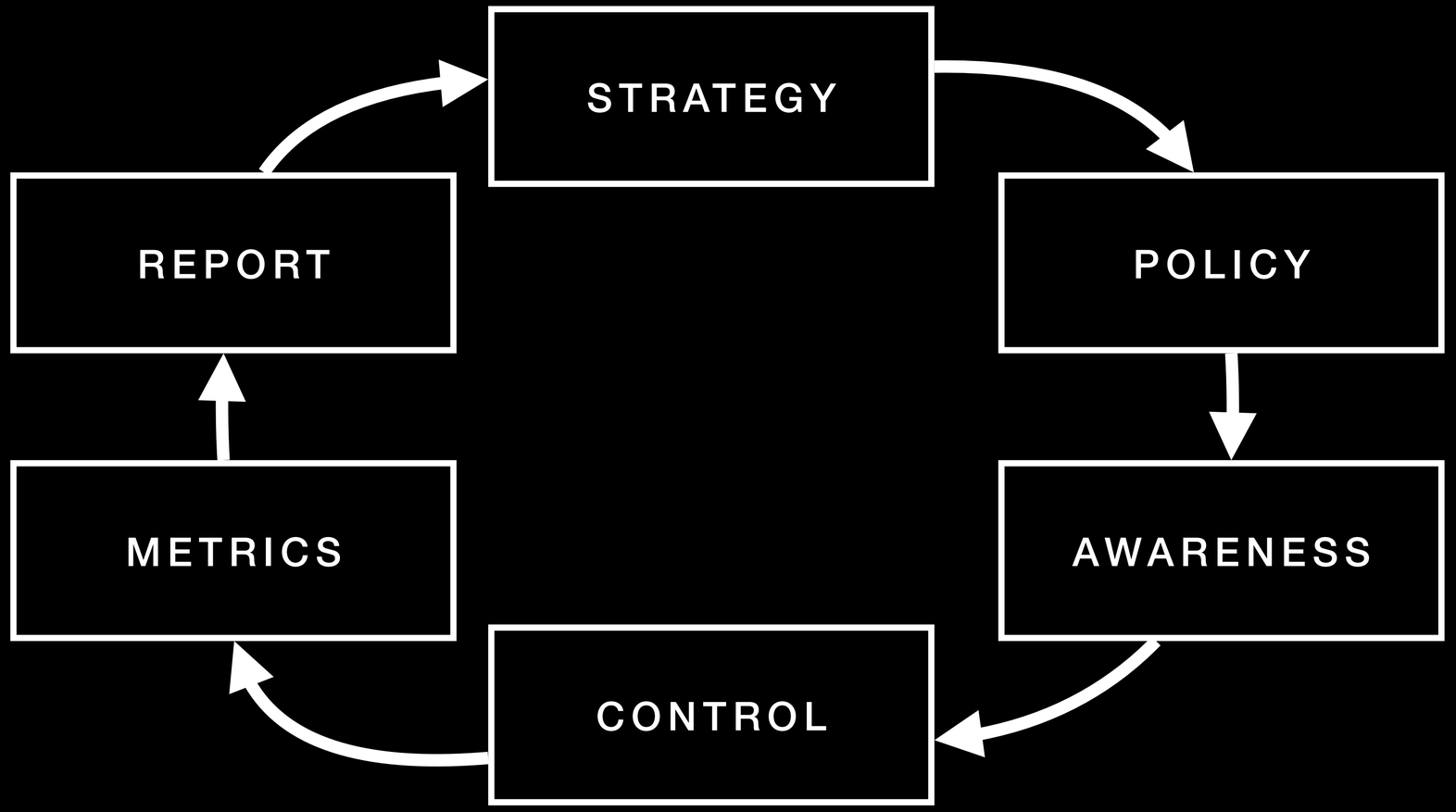
Bayuk, 2007
Cyber Security Management Cycle



Bayuk, 2007
Cyber Security Management Cycle



Bayuk, 2007
Cyber Security Management Cycle



Bayuk, 2007
Cyber Security Management Cycle

Metrics