ENTERPRISE CYBER SECURITY

METRICS

University of Glasgow

METRICS

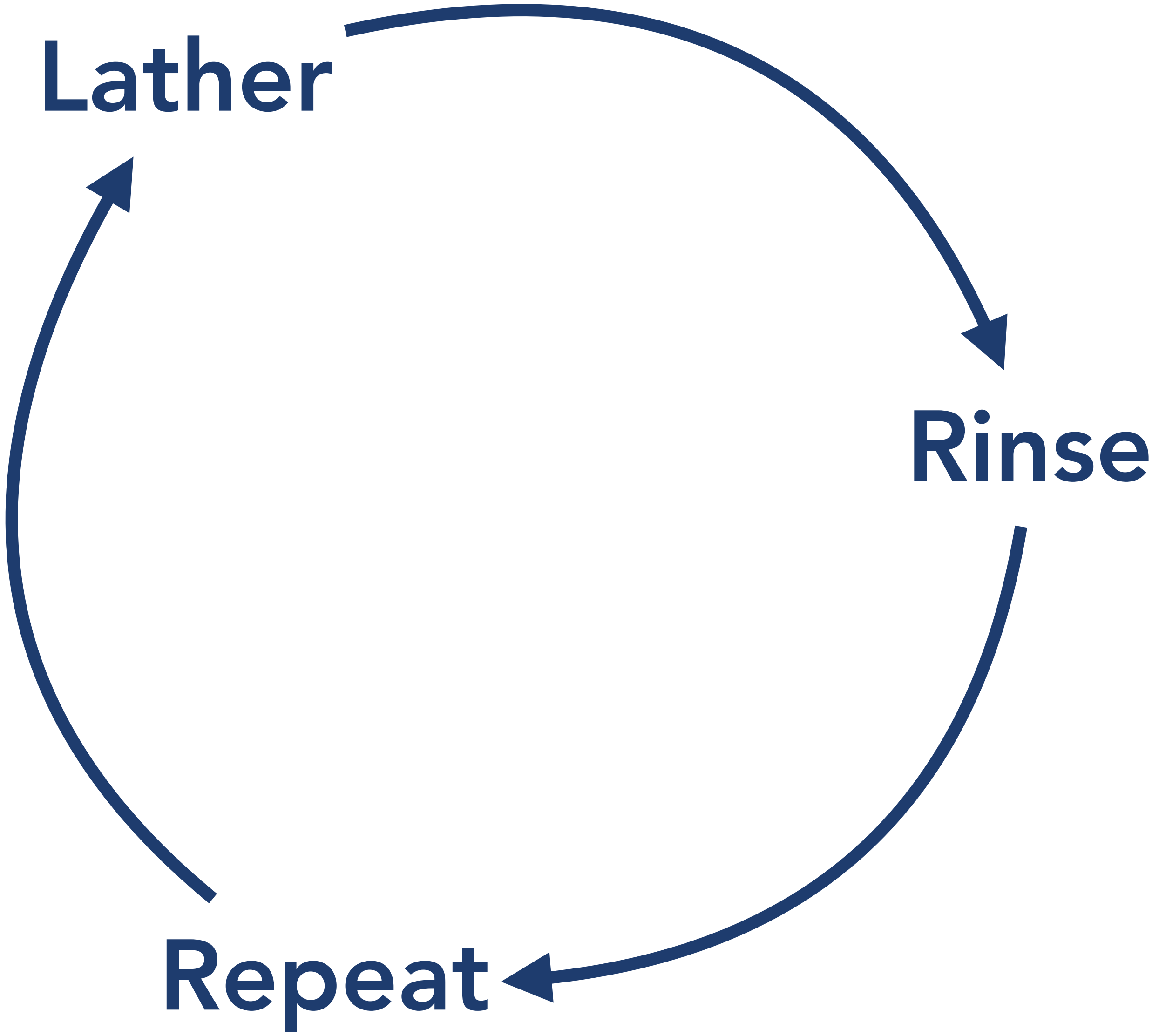
- cyber risk management processes are typically strong in terms of **identification** and **treatment**.

- alternative perspective is that cyber risk management should be strong in **quantification** and **value**.

- **assets** should be considered as well as the risk.

- the concern is that we following the shampoo algorithm, an **endless loop**, but without ever getting clean.

SHAMPOO ALGORITHM



Lather

Rinse

Repeat

QUANTIFYING RISK

- **quantifying** risk is much harder, than identification of risk.
- asset understanding must be established and this requires asking difficult questions.
- not only the **value of the asset**, but the **expense of the controls** as well as **cost comparison** with peers.
- **reaching a consensus** on just a single question can be a challenge.

HOUSE PRICES

HOUSE PRICES GAME

- need to amass panel of experts about Glasgow
- panel about buying a house, panel comprising of different actors.
- potential data source would be the land registry to find out local prices.
- social networks such as Twitter, Facebook etc.

QUANTIFYING RISK

- **quantifying** risk is much harder, than identification and risk.
- assets must be established and this requires asking difficult questions.
- not only the value of the asset, but the **expense of the controls** as well as **cost comparison** with peers.
- **reaching a consensus** on just a single question is a challenge.

CHARACTERISTICS

- communicable across company
- comparable with peers
- contextually specific - so that leaders can make decisions
- expressed as a number, try to avoid qualitative labels

CHARACTERISTICS

- simple to explain
- benchmarking
- time and money
- reliable measurement

SECURITY IS A PROCESS

- recall from the introductory lecture, that security is a **process** and not a **product**.
- many industries are **driven by processes** and any captain of industry knows the **key barometers**.
- these barometers or measurements are **not necessarily obvious**, given the industry.
- many enterprises have large, complex supply chains where **inventory turnover** is one such, key barometer.

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.

MOTIVATION FOR METRICS

- the aim is often 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

- US Government Performance Results Act (GPRA) is example of organisations required to improve performance.
- GPRA expects organisations to define goals, both long and short-term and define performance targets.
- US Federal Information Security Management Act (FISMA) requires organisations to demonstrate controls inline with data being utilised.
- security metrics can be reported as examples of key performance indicators being inline with FISMA.

SHARING CONCERNS

- unlike attackers, enterprises are incredibly poor at **sharing** information about security among themselves.

- poor **market incentives** and slow moving **rules and regulations** that could be used interpret actions as collusions or **require disclosure**, e.g. anti-trust and Freedom of Information.

- no real common language or vocabulary as well as much of the information being **imprecise**.

- often taken from **different perspectives**, producing highly subjective information.

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**.

QUESTIONS

METRIC TYPES (NIST SP800-55)

- different metrics can be used in tandem, but the expectation is that **focus shift as security program evolves**.
- **implementation metrics** offer insight in the adopting of security controls and/or programs.
- **effectiveness and efficiency metrics** offer insight into if a program or control is operating optimally.
- **impact metrics** offer insight into the impact of security controls on specific business objectives.

IMPLEMENTATION METRICS

- designed to offer **insight into the adoption of security improvement programs** and/or **controls**, e.g. percentage of systems configured with approved password approach.

- implementation metrics can also offer insight into **elements within the enterprise**, e.g. percentage of servers with approved configuration.

- implementation metrics will indicate less than 100% initially, but expectation to reach target and **focus on to other metric types**.

EFFICIENCY AND EFFECTIVENESS METRICS

- designed to offer insight in terms of security processes and controls are **operating optimally**.

- **effectiveness** refers to the strength of the control in addressing the perceived security concern, e.g. percentage of security incidents from misconfigured security controls.

- **efficiency** refers to the timely nature of the control, e.g. percentage of servers serviced on schedule.

- efficiency and effectiveness metrics are valuable to key decision makers in determining if controls and policies are operating as expected.

IMPACT METRICS

- offer insight into the impact of security process and controls on an organisation.
- such metrics are tied tightly to the organisation itself and are used to demonstrate impact on potential business objectives.
- such objectives could be demonstrating cost savings from implementation of specific controls.
- could also include demonstrating increased levels of consumer trust with an organisation.

STRONG METRICS

STRONG METRICS

- **empower** individuals by being **specific** to a given context.
- are **transparent** and **verifiable** measurements.
- are expressed **numerically**.
- should be **timely** and relevant.
- **inexpensive** to collect.

TRANSPARENT AND VERIFIABLE MEASUREMENTS

- subjective ratings, such as `very high' or `low', are easily altered depending on the instrument.

- experts may differ, indeed others may simply lack knowledge and experience.

- the same **outcome** should be expected in the same process is followed.

- the process should be clearly **documented**, inviting understanding and criticism.

- metrics that are **cumbersome** or **complex** only invite doubt and distrust, worse they can be **misleading**.

TIMELY AND INEXPENSIVE

- security process decisions should be ideally **considered frequently**, rather than annually.
- metrics should be **inexpensive to obtain**, resulting in them being collected frequently.
- aim is to **avoid metrics that are complex to produce**, involving elaborate procedures, staff time and resources.
- ideally metrics should be **collected automatically** supporting more timely decisions.

NUMERICAL

- strong metrics are often expressed **numerically**.
- **percentages** or **cardinal numbers** are good examples, not ordinal numbers.
- strong metrics are associated with a unit of measurement, for example ‘incorrect password entry for a given system’.
- possible to generate multiple units of measurement, for example ‘how many predictable passwords per 1000’.

CONTEXT

- metrics support strong decision-making, context considered metrics mean something to those making decisions.
- reflecting the needs of specific elements of the business.
- generic metrics for the entire organisation may support simple decisions, but have little meaning for specific units.
- consider threats to systems on campus, versus threats to systems used by registry staff.

WEAK METRICS

WEAK METRICS

- weak metrics are unsurprisingly metrics that do not exhibit the characterises of strong metrics.

- they are **inconsistently measured**, leading to subjective data that could vary between measurements.

- **expensive to gather** and **slow to produce** due to the expensive of collection.

- **difficult to express**, but relying on ordinal numbers or other rating approaches is **not wholly negative**.

POOR MEASUREMENT

- qualitative data is important, but does not necessarily make a strong metric.

- human judgement is **subjective** and could easily differ between the individuals making the judgement.

- subjective ratings could also suffer from **bias** or **differences in knowledge**.

EXPENSIVE AND COMPLEX GENERATION

- complex generation processes may result in poor understanding of how the metric is produced.
- lack of understanding of generation can result in poor decision making.
- some metrics or data can only be produced from laborious activities (e.g. FOI requests).
- if the metric is expensive to collect or generate, it could result in longer sampling windows.

DIFFICULT TO EXPRESS

- typically not expressed numerically and do not represent a unit of measurement.

- do not represent quantity, more likely to represent a **rating**.

- labels such as 'high', 'medium' and 'low' may have value, but do not make strong metrics.

- such measurements are beneficial when complimenting a stronger metric.

DIAGNOSING PROBLEMS

METRICS TO DETERMINE A PROBLEM

- conducted much the same way as research
- produce a hypothesis or research questions
- we construct a methodology and produce test to accept or reject our hypothesis
- we attempt extract values for these, in terms of metrics we may do this numerically
- discuss and conclude and determine if the evidence in measurements supports rejecting the null hypothesis

SECURITY METRICS CAN HELP

- understand the problem
- see emerging issues
- understand the potential weakness in the infrastructure
- measure performance and countermeasure
- recommend additional technology or process improvements

AREAS TO CONSIDER

- perimeter defences
- coverage and control
- availability and reliability

PERIMETER DEFENCES

PERIMETER

- recall from previous lectures that enterprises traditionally focused on their own perimeter.

- as systems evolved and enterprises embraced cyberspaces the perimeter became harder to determine.

- areas of interest include communication in terms of email messages coming into internal systems.

- defence against spam and virus transmitted into the enterprise, previous concern was coming in via floppy disk.

EMAIL

- many metrics already associated with email in other domains, such as marketing (e.g. open rate and subscriptions per subscribe).
- governments among other organisation use these metrics to understand the impact of email on citizens
- similarly, metrics trying to understand perimeter defences in terms of email
- spam detected for example may be good at telling if its growing - but its not necessarily valuable
- maybe better to look at false positives and false negatives.

EMAIL

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

- viruses are common, traditionally passed through floppy discs now over the network

- many email systems come with content filtering solutions, but we will want to understand what ones require manual cleaning

- also want to understand how many virus have been quarantined and then overridden by the users (e.g. APTs).

- also need to consider the impact the internal network is having on the external network (e.g. outbound viruses).

VIRUSES

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

COVERAGE AND CONTROL

COVERAGE AND CONTROL

- insight into the coverage or **implementation** of program or specific controls.
- organisations want to be able to demonstrate coverage of security programs and controls.
- insight into the control or **effectiveness** of the controls in place.
- ability to implement controls, means little if the controls themselves are not effective.

COVERAGE AND CONTROL

- **patch management** of enterprise systems to ensure that security fixes are deployed in a controlled manner.

- **system configuration** of enterprise components to ensure systems are not exposed to specific vulnerabilities.

PATCH MANAGEMENT

- software patches can effectively **alter** or **modify** program code to mitigate against specific threats.

- organisation needs to have an understanding of assets and the relevant patches.

- important to remember **several systems are being altered** that individuals use everyday to achieve business objectives.

- established **patch cycle** that can be coordinated between company and providers as well as being based on time and priority (e.g. Microsoft 30-day, Patch Tuesday and Exploit Wednesday).

- **prioritising** in terms of threats that may be addressed and **scheduling** by ensuring critical systems are not unavailable because they are being updated.

PATCH MANAGEMENT

- **test patch** within a controlled environment to determine any issues or conflicts.

- consider slow **rollout** of patches to different zones to determine any conflicts.

- patches need to handled through **change management** with proper consider contingency plans incase blackouts occurs.

- **organised** and **controlled** patch installation process to ensure smooth continuity of the system as a whole (e.g. consider some units performing differently from others).

PATCH MANAGEMENT

- **audit** and **assess** the success of patch management to understand the level of coverage and control.

- determine the level of **coverage** and what systems should be patched.

- similarly, determine if the systems that should have been patched, have been patched.

- ensure **consistency** across all units and **compliance** after the installation of patches.

PATCH MANAGEMENT

- routine patch management **does not necessarily improve security**, but poor security could come from poor patch management.
- effective patch management does **demonstrate a strong security program** in terms of coverage as well as control.
- patch management can be **expensive** in terms of workload to staff, consider manual updates to several systems.
- potentially **workload heavy** in terms of actually determining the requirements of different systems (e.g. critical servers vs. workstations).

PATCH MANAGEMENT

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

SYSTEM CONFIGURATION

- consider the configuration of the individual systems connected to the cyber space.
- tailor system configuration to that of the organisation and business objectives.
- enterprise should avoid off the shelf configuration, useful metric may be to understand expense in terms of reconfiguration.
- useful to also understand the number of systems configured to industry best practice.

SYSTEM CONFIGURATION

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

AVAILABILITY AND RELIABILITY

AVAILABILITY

- **uptime** of elements within the enterprise, if they are not available business process may not be able to complete.
- **recovery** of elements within the enterprise to ensure they can be brought back online after failure or compromise.
- **change control** of elements to ensure they are taken offline in a manageable manner.

UPTIME

- **uptime** is typically consider the time a resource is available and accessible.
- enterprises and organisations want to **ensure resources are available when needed.**
- **planned downtime** is when a system is effectively not available and organisation use this to alter and maintain resources.
- **unplanned downtime** is when systems are unexpectedly unavailable, possible due to compromise or non-malicious activity.

UPTIME

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

RECOVERY

- enterprises need to understand how **resilient systems** are after an attack or unplanned downtime.

- need to have an understanding of the average time it takes an organisation to get an **inoperable resource available again**.

- enterprises need to **plan for disaster recovery**, ensuring plans are in place to restore critical assets.

- **rehearsals of disaster recovery plans** need to performed to determine any optimisations or issues.

RECOVERY

METRIC	MOTIVE	SOURCE
SUPPORT RESPONSE TIME (TIME)	MEAN TIME FOR RESPONSE	BOOK KEEPING AND SPREADSHEETS
MEAN TO RECOVERY (TIME)	INSIGHT INTO THE TIME TAKEN TO RECOVER	BOOK KEEPING AND SPREADSHEETS
ELAPSED TIME SINCE (TIME)	INSIGHT INTO HOW THE ORGANISATION CAN RECOVER	BOOK KEEPING AND SPREADSHEETS
ELAPSED BUSINESS CRITICAL SYSTEMS (TIME)	NIGHT INTO HOW THE ORGANISATION CAN RECOVER ON CRITICAL COMPONENTS	BOOK KEEPING AND SPREADSHEETS

CHANGE MANAGEMENT

- enterprises need to ensure an effective program of change management, alterations must be planned, managed and documented.

- organisations want to ensure that alterations are not applied to production systems without prior approval.

- ad-hoc alterations could led to unplanned downtime and significant expense for an enterprise.

- enterprises also want to ensure alterations are made during low activity periods or during planned downtime.

CHANGE MANAGEMENT

METRIC	FOCUS	SOURCE
NUMBER OF CHANGES (COUNT)	UNDERSTANDING NUMBER OF CHANGES IN PRODUCTION CONTEXT	CHANGE MANAGEMENT SOFTWARE
CHANGE CONTROL EXEMPTIONS PER PERIOD (%, COUNT)	EXCEPTIONS THAT ARE MADE FOR CHANGES OUTSIDE NORMAL MANAGEMENT	BOOK KEEPING AND CHANGE MANAGEMENT SOFTWARE
CHANGE CONTROL VIOLATIONS PER PERIOD (%, COUNT)	VIOLATIONS OUTSIDE NORMAL MANAGEMENT	BOOK KEEPING AND CHANGE MANAGEMENT SOFTWARE
CHANGE CONTROL VIOLATIONS BY BUSINESS UNIT PER PERIOD (%, COUNT)	VIOLATIONS OUTSIDE NORMAL MANAGEMENT BY BUSINESS UNIT	BOOK KEEPING AND CHANGE MANAGEMENT SOFTWARE

PROBLEMS WITH METRICS

Sample Copy
Clear/Stop
C/⊘
Start
Enter
#
0
6
9
8
5

COCA-COLA EXAMPLE

MEASUREMENTS

- starting point was to suggest that risk assessment is good at identifying risks but not good at quantification.
- risk management is all about dealing with uncertainty and unpredictability.
- measurements and numbers do not always give a complete story.
- numbers can be interpreted, manipulated and discussed out of context.

MIND THE GAP

- potential for gaps in coverage and lack of understanding for some areas of the organisation.

- temptation may be to focus on other areas where there are significant areas of improvement.

- solution is to understand the gaps and close them.

- careful consideration must be made to ensure that the number of metrics does not become unwieldily.

STRIVING FOR SCIENCE

- strong metrics should be expressed numerically and should not be subjective.
- concludes that ratings that are subjective are worthless, even dangerous.
- motivation for metrics remember is to support strong decision making - management and decision making are not necessarily scientific.
- exercising caution when diminishing data or opinion that may not consider scientific.

NOT METRICS

- metrics that are **inexpensive and easy** to obtain, may not represent any real value to making better decisions.
- number of **vulnerabilities resolved** may not be of any to many decision makers when we consider it does not necessarily give an insight into future vulnerability counts.
- **viruses detected** is unlikely to be of any interest to anyone outside the providers of virus detection software.
- **inbound spam** count seems irrelevant as an organisation has little control of the spam coming in.

NOT METRICS

- insight into **compliance is important**, but strict focus on compliance could be to the detriment to an organisation.

- **commonly used metrics** are not necessarily the best metrics for a specific enterprise.

- metrics need to be tailored to the objectives of the organisation and considered with a question in mind.

OVERVIEW

- considered the concept of metrics and the characteristics of them.
- identified what represents a strong and weak metrics as well as how they can be used in diagnosis of problem.
- discussed the limitations of metrics and the problems on relying on them exclusively.