ENTERPRISE CYBER SECURITY

POLICY

University of Glasgow

CYBER SPACE AND SYSTEMS

- cyber systems and space have **empowered enterprises** and individuals to be more effective and competitive.

- potential for cyber space and systems is unparalleled if enterprises are able to **rely on them**.

- enterprises need to ensure cyber security and have **confidence** in the systems and spaces they rely on.

- recall the **tenants of cyber security** from the first lecture.

TENANTS OF CYBER SECURITY

- **prevent**, **detect**, **respond** - consider emergency services as an example.

- **people**, **process**, **technology** - security is the responsibility of everyone not just professionals.

- **confidentiality**, **integrity** and **availability** - information security important to enterprises.

TENSION

- cyber systems and spaces offer amazing **opportunities and flexibility**.

- **empowering disruption** of numerous markets and delivering more for consumers.

- problems arise with the deployment and use of cyber space, specifically **security** concerns.

- cyber security policy can be considered an approach to mediate the **tension between demands of both**.

AMBIGUOUS

- policy can mean many different things, especially when considered from **different perspectives**.

- policy could refer to laws and regulations, enterprise cyber security objectives, configuration guidance as well as operational guidance.

- unfortunately such **ambiguity exists throughout cyber security**, multiple definitions and perspectives.

- cyber security policy can be considered **directives to ensure cyber security**.

POLICY

- cyber security policy can be considered the **codification of cyber security objectives** to support desired behaviour to achieve said objectives.

- objectives do not **easily translate** into specific behaviours.

- standards and best practice can be used to **comply with policy**, but standards are not themselves policies.

- standards may be recommended that are not associated with policy and policy may have not be associated with standards.

POLICY

- policies provide the blueprint for the overall cyber security approach for your organisation.
- policies are not procedures, they do not prescribe specific implementation details.
- policies present security goals, rather than specifications.
- policies may require the documentation of implementation, but implementation should not form part of policy.

SIGNIFICANCE

- cyber security is the **responsibility of everyone**, not a single entity or individual.

- cyber security objectives should be achieved by everyone behaving in the desired fashion.

- policy offers guidance to employees and other stakeholders.

- **management must demonstrate strong support** for policy otherwise it will be ignored.

LIABILITY

- cyber security policy takes **business processes into consideration** and wants to protect them.

- information has become **crucial** to many different business processes.

- **insurance companies** will want to understand if policy has been developed.

- aim is to **reduce the liability** an enterprises is exposed from not properly understanding assets, risks and processes.

COHERENT NARRATIVE

- **complexity** of enterprises ensures it can be difficult to maintain a coherent narrative across every aspect of cyber security.

- policy becomes useful tool in supporting a coherent narrative across the enterprise.

- elements can come and go within the larger system and the same objectives should be achieved.

QUALITY AND COMPLIANCE

- enterprises must ensure there business processes operate within the framework of the environment.

- consider the laws and regulations of previous sessions, even external entities must demonstrate compliance.

- enterprises will seek to demonstrate quality control of processes, e.g. ISO9001.

- policies can be valuable artefacts in determining what is working and what is not working.

POLICY

GOVERNANCE

GOVERNANCE

- several enterprises **collapsed** within the United Kingdom in the 1980s.

- **questioned the approach to management and governance** of many organisations.

- Bank of Credit and Commerce International (BCCI) was **forced to closed** due to poor management.

- 1992 **Cadbury Report** made several recommendations to minimise the threats to assets through poor management.

GOVERNANCE

- policy aims will alter inline with the **governing body**.
- policy is **governed by a given group** and applies to a specific realm, for example state vs enterprise.
- policy producing process will also be **influenced** by the governing body, for example state, enterprise and university.
- many policies may be **governed by different units** within an organisation, potentially creating **conflicts** and **overlaps**.

REGULATION

- **policies are not laws**, but at state level they can influence regulation creation, for example UK exit from EU.

- laws and directives can be produced **without policy**.

- China has the policy that the **Internet is to serve the objectives of the state** - leading to the creation of specific laws.

- EU outline the policy that the Internet should be **open and accessible** to all and to market that beyond the EU.

- policy is restricted to the governing realm and gaps could emerge between domains.

CHINA VS EU

SMALL GROUP DISCUSSION

CHINA VS EU

- consider the different **policy positions** of China and the EU regards cyberspace or the Internet.

- **security implications** in terms of the authorities defending nations against national threats.

- **predict** some of the social issues that may arise from such policy.

INVESTIGATORY POWERS BILL (UK)

- designed to support UK intelligence agencies as well as law enforcement.

- collection of communications data to support investigation into individuals and entities.

- includes extending some of these powers to local government to investigate fraudulent behaviour.

- require communication service providers (CSPs) to retain communication transactions for 12 months.

CHINA VS EU

- China and EU clearly have very different policies on cyberspace and the Internet.
- UK is able to create laws that still allow it to defend against national threats and do not clash with policy.
- if anything, the policy position of the EU, potentially supports greater security as the UK has more information.
- in a way the policy of the EU is serving the governance of UK well.

ENTERPRISE

- enterprises and organisations can **enforce** policy, much like laws.

- failure to **comply** with policies can led to retraining or even termination, but such **response must be legal**.

- scope is still limited to the governing body, business units may have policies, but these will be limited to the specific domain.

- cyber security is not necessarily perceived by many organisations as a **great office of state**.

ENTERPRISE

- cyber security policy may be the remit of the support or technology unit.

- concern is that such policies may be altered to suits the perceived needs of the individuals.

- consider a sales concern, purchasing a product that may in turn undermine the security of the organisation.

- consider finance, individual employees are not able to determine what is an expense, and what is not.

SYSTEM OPERATIONS

- enterprises may adopt standards to comply with regulatory requirements of the state.

- standards and recommended processes may be labelled as security policy.

- scope may be restricted to specific platforms or processes and not extended beyond.

- concessions may be made to utilise a specific technology platform or even overlap between different business units.

SYSTEM CONFIGURATION

- system configuration is important to ensure consistency across the enterprise and is important to coverage and control.

- enterprises tend to adopt recommended or standard set of configurations.

- standard or recommended configurations may be outlined by product vendors and become known as policy.

- mindful that the goals of vendors are not necessarily the goals of the enterprise, e.g. Apple Inc. and Adobe Flash.

POLICY

STRATEGY

STRATEGY

- policy communicates the cyber security strategy for the enterprise.
- management objectives that be used to determine appropriate measures.
- standards, provided by organisations such as ISO and NIST, inform and guide policy development, but are not in themselves policies.
- recall policies are not implementation specifics and do not necessarily represent the optimal solution resulting in unforeseen consequences.

FORMATION

1. decisions pertaining to cyber security can occur without a policy being in place.

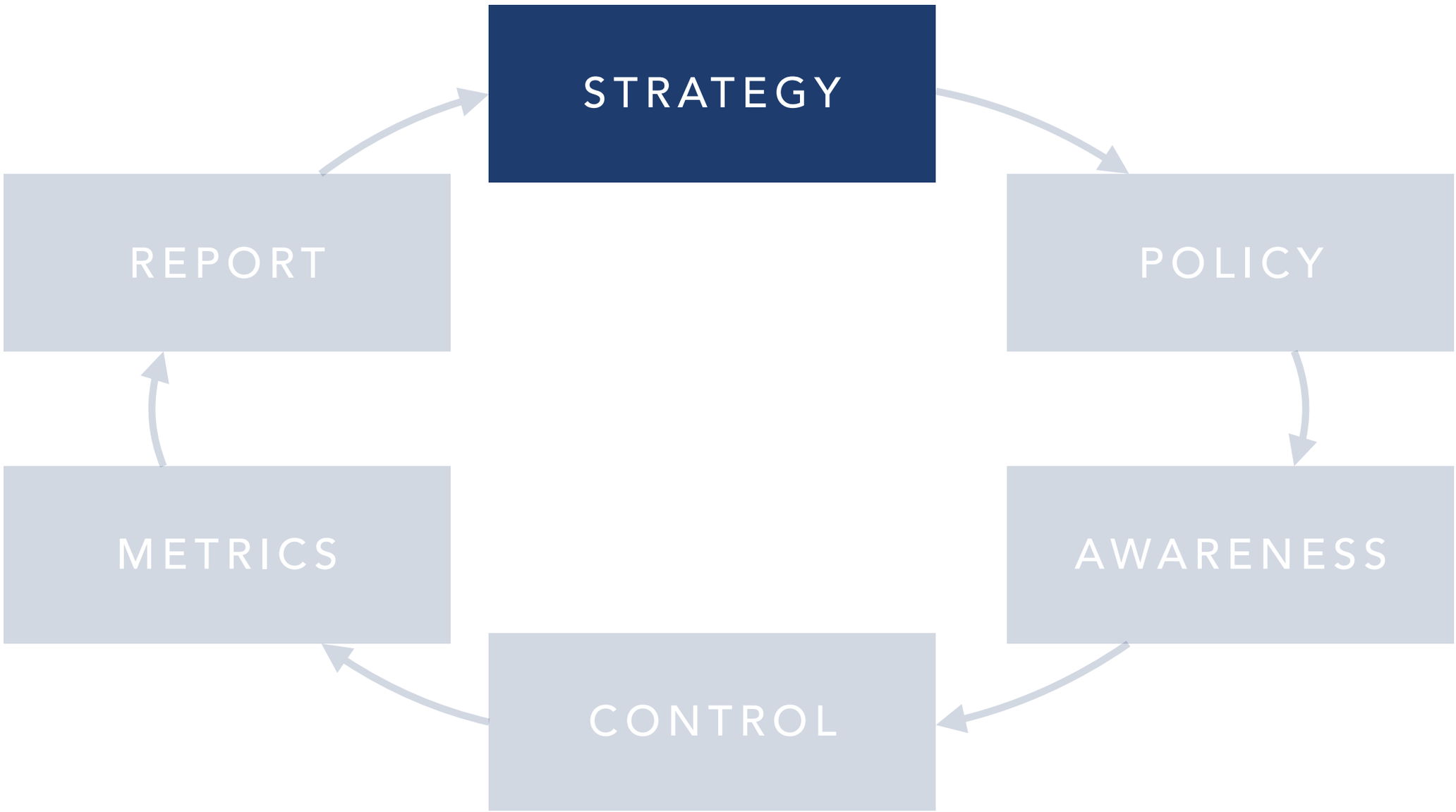
2. cyber security policy is a valuable tool in directing decisions pertaining to cyber security

3. understanding what informs and guides security decisions.

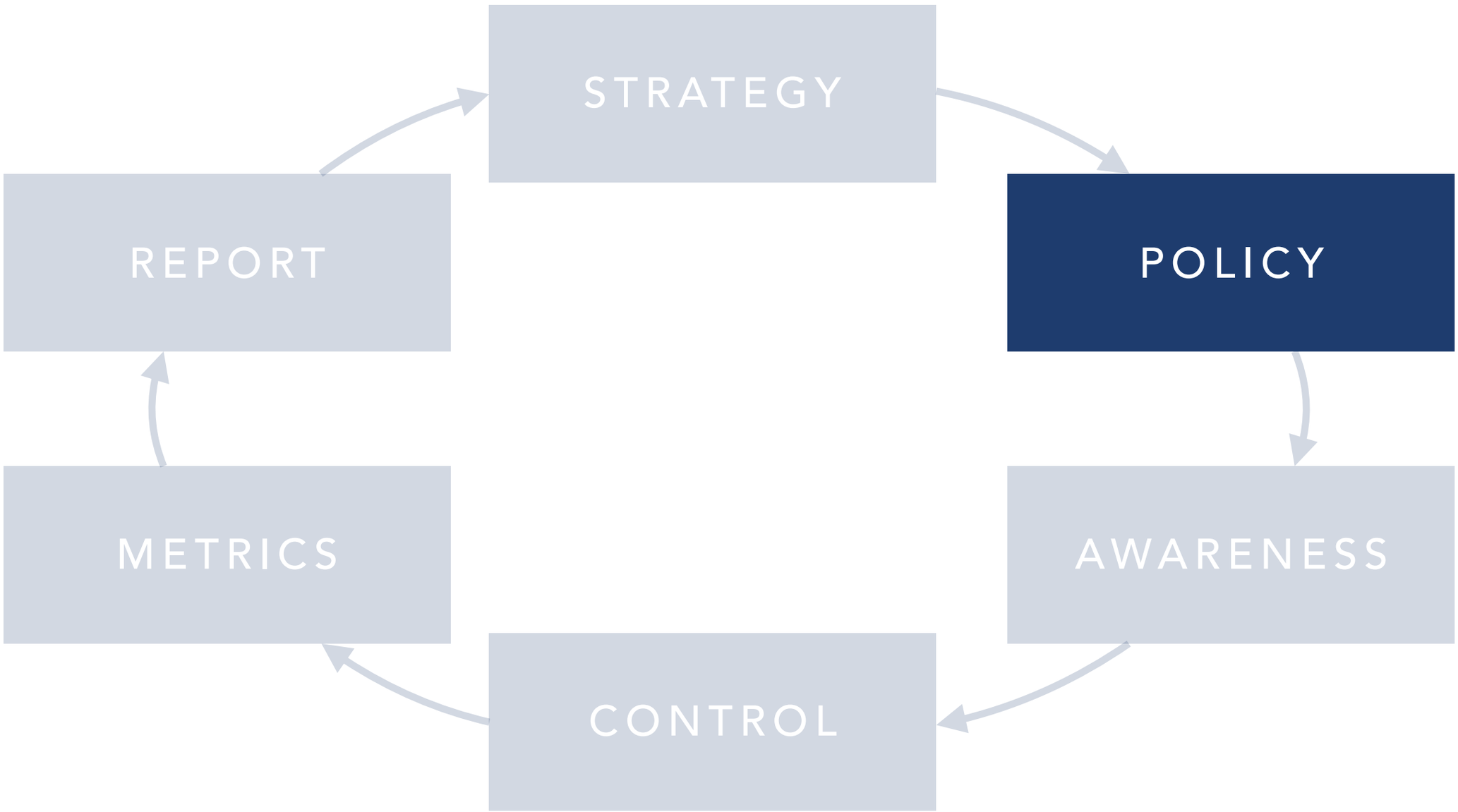
STRATEGY

- policy is a key component of cyber security management.
- policy communicates strategy and informs individuals employees of things are done.
- enforcement solutions and monitoring can be used to manage cyber security objectives.
- monitoring should inform the success of enforcement as well as future revisions of strategy.

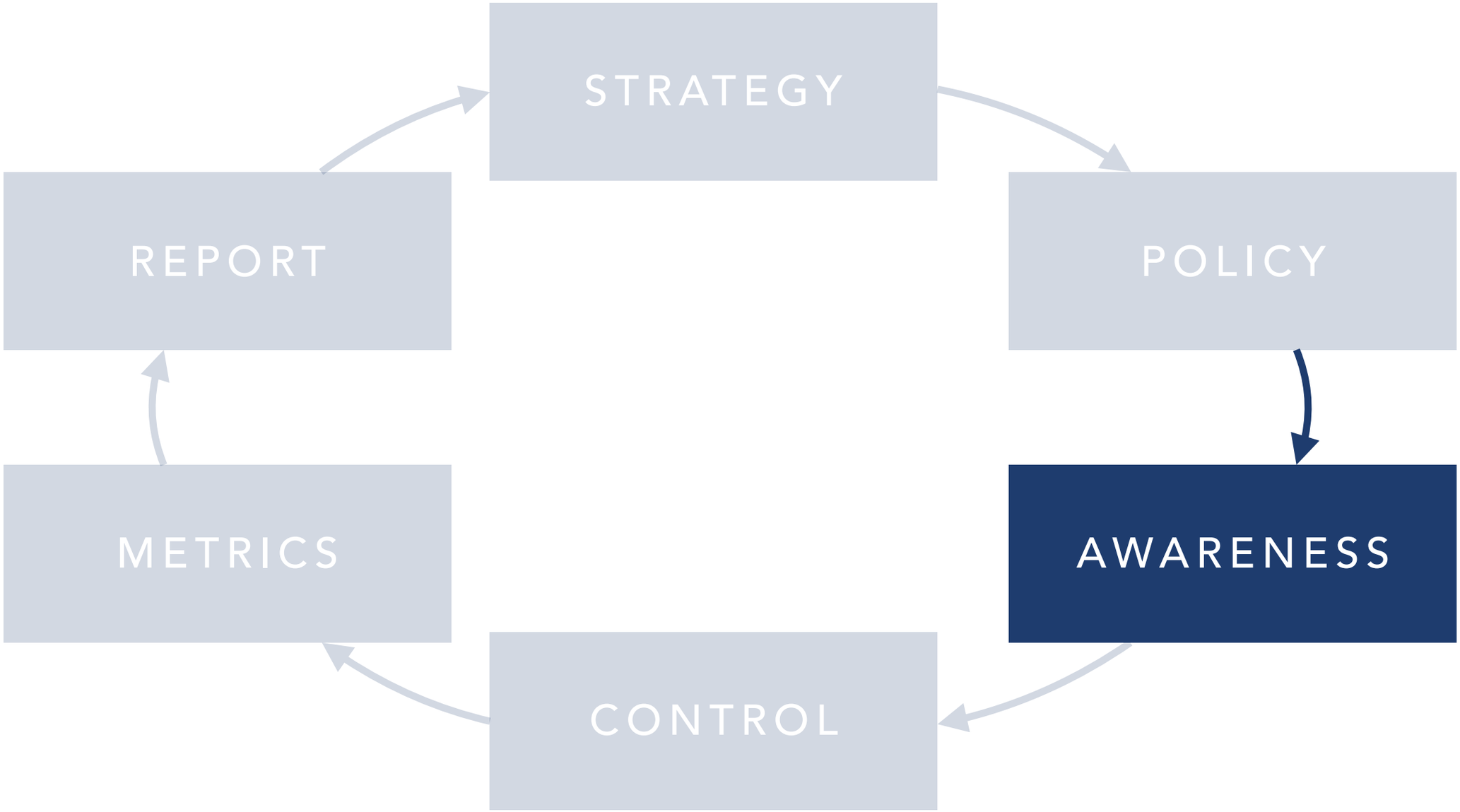
CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



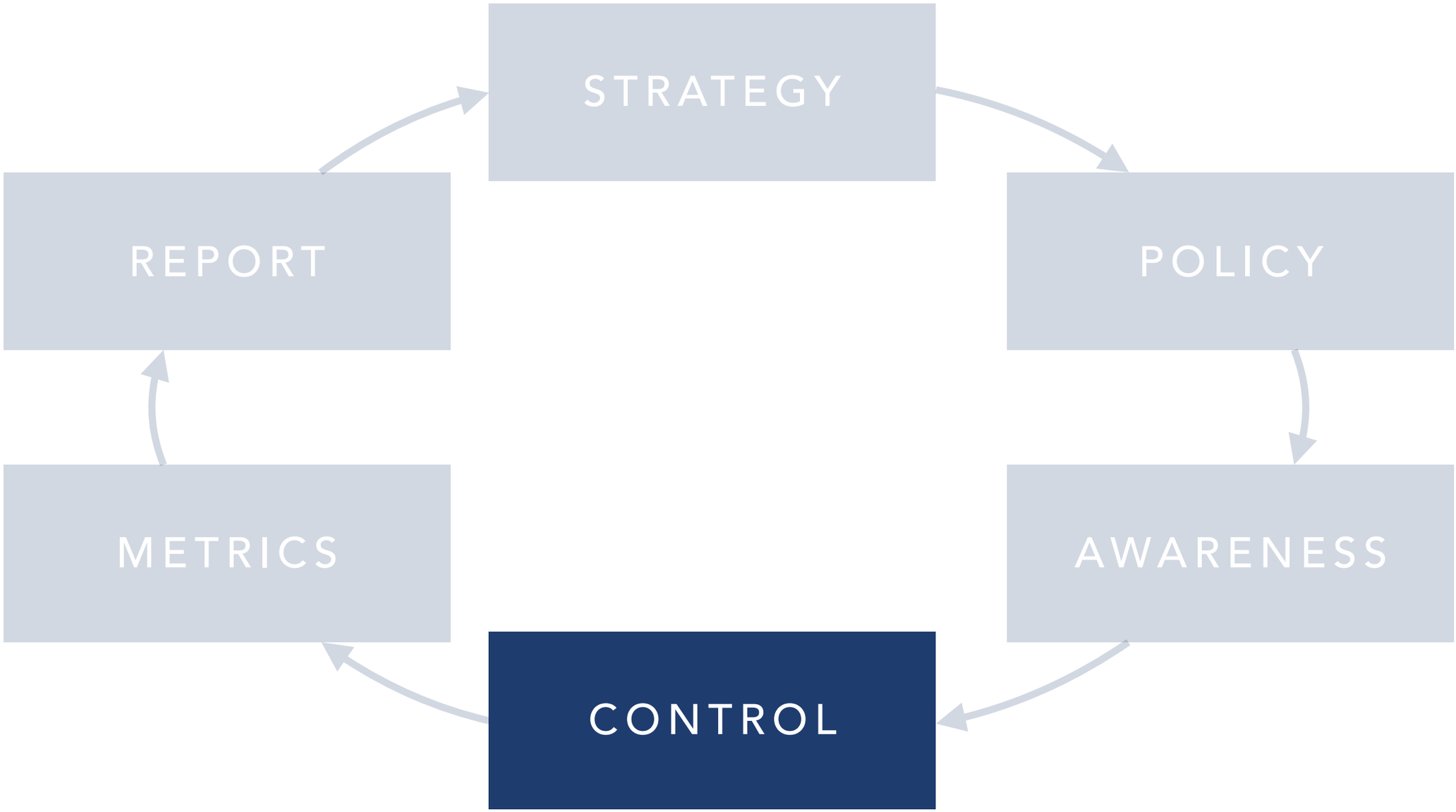
CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



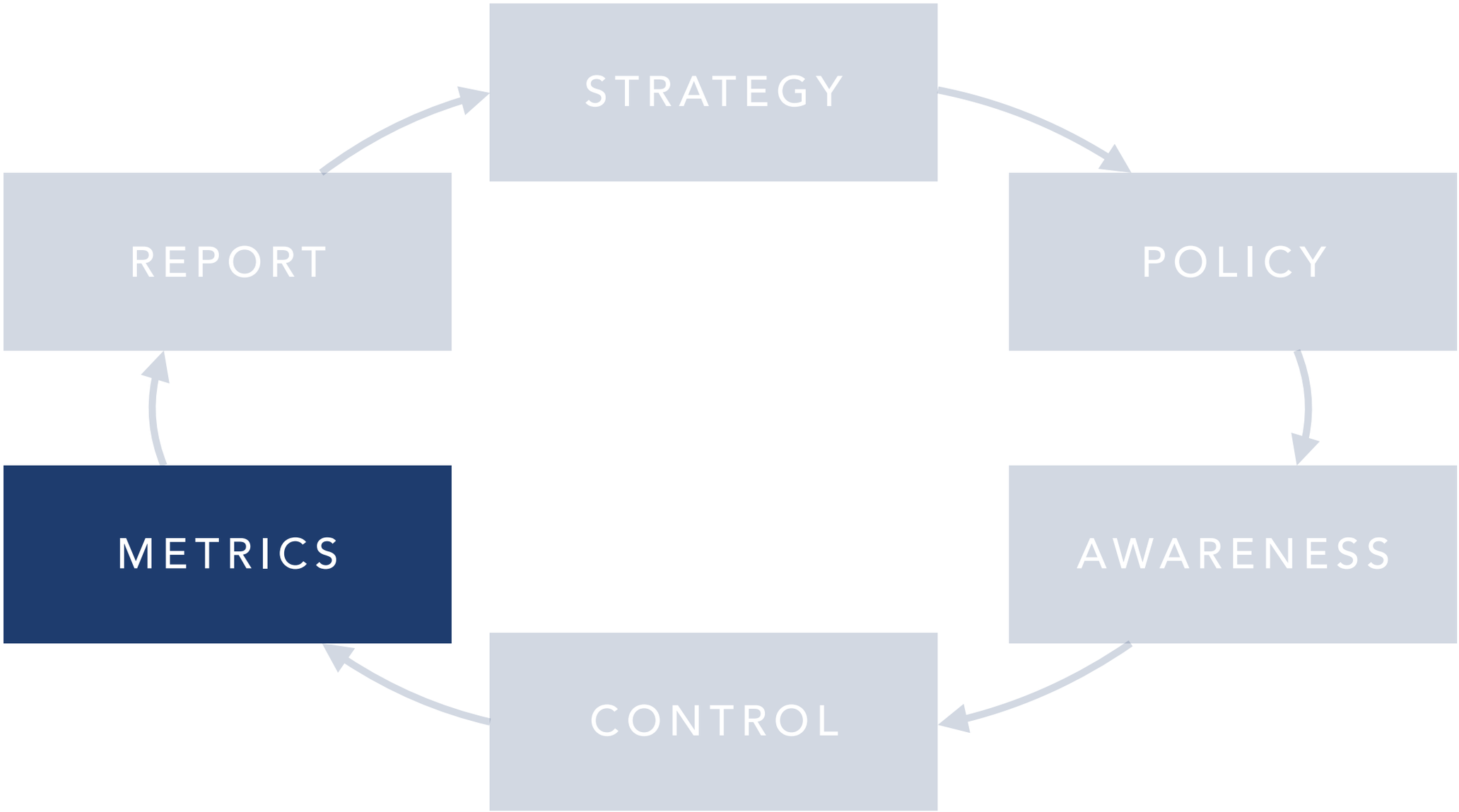
CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



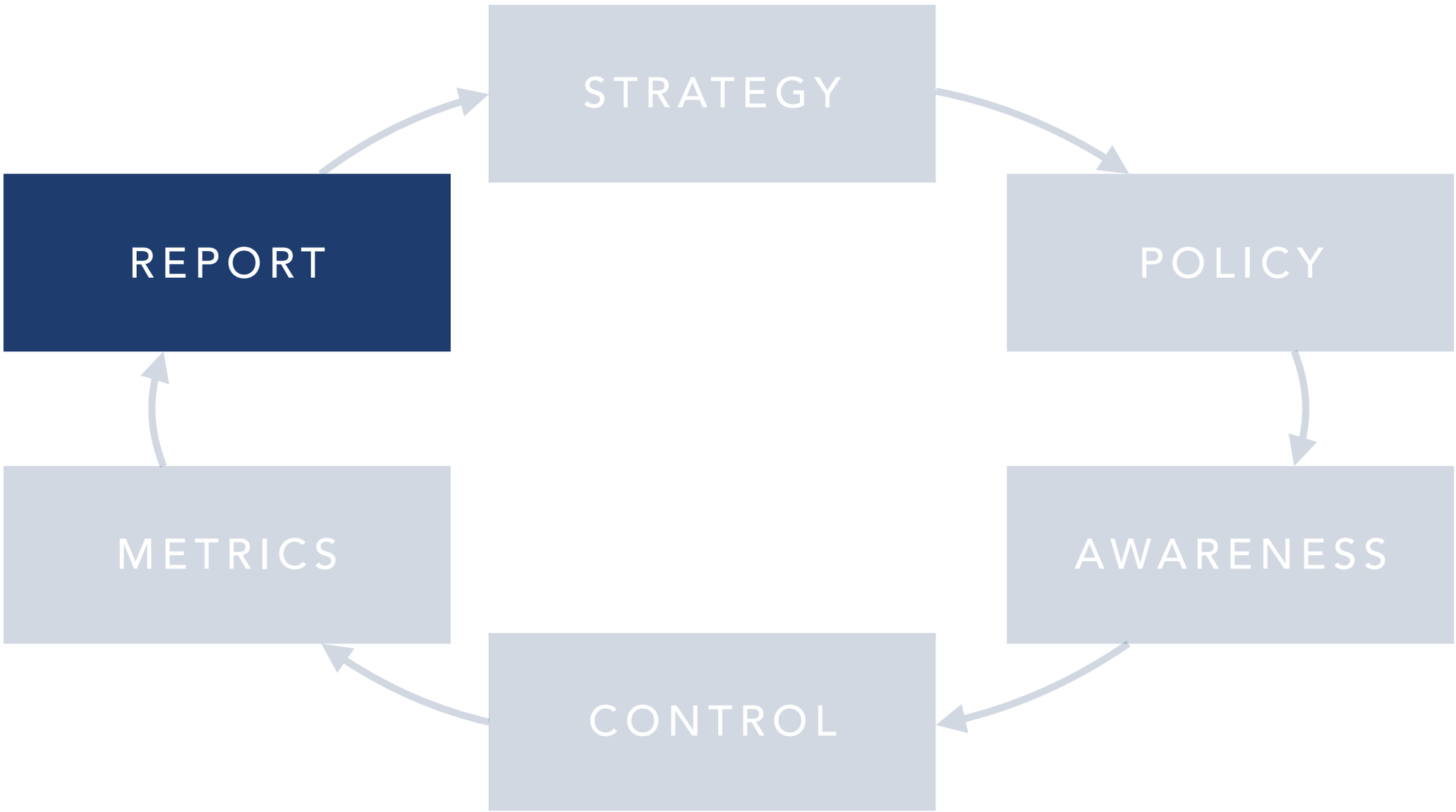
CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



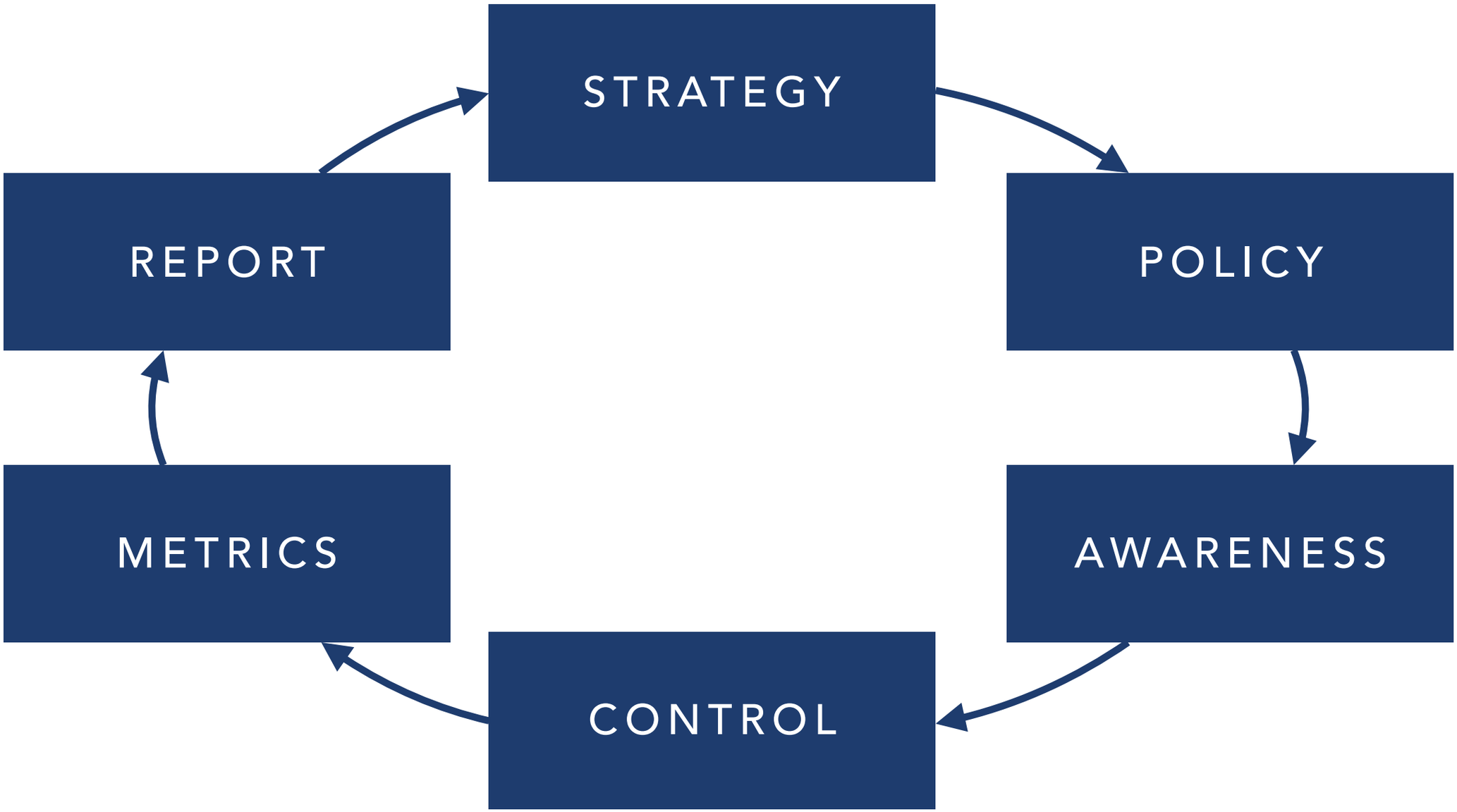
CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



CYBER SECURITY MANAGEMENT CYCLE (BAYUK, 2007)



DEVELOPMENT

PURPOSE

- policies can be produced to mitigate risks for **any number of elements**, including people, process, hardware and software.

- determine the **important resources** to the enterprise and the policies required.

- many **different approaches**, possibility is a policy document with many chapters or several policies for many different units.

- the aim to communicate a strategy, gain management support and create awareness - effectively try and keep it **concise** and **clear**.

TIMING

- policies should be produced before security issues emerge.
- policy is far more straight forward while systems are being designed and developed, rather than retrofitting.
- development after a security failure is possible, problems could still be avoided.

APPROACH

- understand what are the actual resources and processes that the organisation is trying to protect.

- determine what it is trying to protect these **assets** and **processes** from.

- ideally develop policy **before threats emerge** and compromise the assets of the enterprise.

- **verify and validate** policy in subsequent reviews to ensure it is meeting the need of the enterprise.

METHODS

- perform **cyber risk analysis** of the enterprise to gain deeper understanding.
- conduct an audit and take **inventory of resources**.
- utilise **frameworks** for given domains and professions to guide policy development.
- adopt recommended **standards** and **processes** for a current domain or organisation.
- consult **vulnerabilities data sources** and perform research analysis of current concerns for the domain.

CYBER RISK ASSESSMENT

CYBER RISK ASSESSMENT

- context is a crucial output from cyber risk assessment that informs of the organisation and environment of operation.

- perform risk assessment and the outputs can inform policy development.

- internal employees should be used to gain insight into business processes and important resources.

- external risk assessment may be advised to ensure an accurate analysis.

INVENTORY

BUSINESS PROCESSES

- understand the activities required to achieve business objectives.

- many different processes, including management, operation and auxiliary processes.

- enterprises need to ensure these processes are able to execute, otherwise objectives will be missed.

- data flow mapping is valuable in understanding valuable elements with the organisation.

"One man draws out the wire, another straights it, a third cuts it, a fourth points it, a fifth grinds it at the top for receiving the head: to make the head requires two or three distinct operations: to put it on is a particular business, to whiten the pins is another ... and the important business of making a pin is, in this manner, divided into about eighteen distinct operations, which in some manufactories are all performed by distinct hands, though in others the same man will sometime perform two or three of them"

– ADAM SMITH, 1776

EQUIPMENT

- enterprises invest in hardware and software to perform business processes and attain objectives.

- understand the business processes and the equipment they rely upon.

- produce an inventory workstations, laptops, printers, mobile devices as well as software programs and tools.

- understand the importance of such equipment to the business processes.

HUMAN RESOURCES

- understand the individuals involved in the **business processes**.
- determine the **business units** involved in the processes themselves.
- understand the **actors** that touch the processes and connection to the enterprise.
- increasingly enterprise outsource and rely on **contractors** and external organisation to perform business processes.
- understand cyber security **roles and responsibilities** of all employees, including external entities.

VULNERABILITY DATA STORES

VULNERABILITY DATA STORES

- **National Vulnerability Database (NVB)**, United States initiative, to produce structured data for known vulnerabilities.

- publishes the **Common Vulnerability Enumeration (CVE)** coupled with data pertaining to level of risk based on use and remedy.

- the aim here is essentially list vulnerabilities in the aim to fix and address them.

- data sharing of flaws has been difficult, especially among security product providers - many of them may use different names for the same vulnerabilities.

VULNERABILITY DATA STORES

- **Common Malware Enumeration (CME)** also eventually published to understand the malware taking advantage of vulnerabilities.

- **Common Weakness Enumeration (CWE)** used to publish software development mistakes that led to vulnerabilities.

- mirrors the idea of the National Quality Forum medical Never-Events, effectively medical mistakes that can be easily avoided.

- NVB was brought down by an attack, actors were able to gain administrative controls of relevant servers.

NEVER EVENTS LIST (US)

- Artificial insemination with the wrong donor sperm or donor egg

- Unintended retention of a foreign body in a patient after surgery or other procedure

- Surgery performed on the wrong body part

FRAMEWORKS, STANDARDS AND PROCESSES

FRAMEWORKS

- essentially **guidance**, effectively **standards** and **best practice**, on how to best mitigate and manage risk (e.g NIST Framework for Improving Critical Infrastructure Cybersecurity).

- typically structured to highlight the areas of strength for an organisation and areas of weakness (e.g. enterprise may be good at identification of risks, but poor at communication).

- frameworks are typically generic and potentially simplistic, not tailored to domain-specific needs.

DOMAINS

DOMAINS

- enterprises vary in terms of function, meaning risk varies between enterprises (e.g. commerce, industrial control and mobile devices).

- generic frameworks, standards and best practices may be the base of a strong foundation, but tailoring must still happen.

- the focus is attain business objectives, through key process, need to ensure process are resilient to risk.

COMMERCE

- digital commerce is common-place with many individuals now purchasing physical and digital goods through the Internet.

- **information is central to this operation**, ensuring it is correct and available for individuals to make purchasing decisions.

- a central business process will be the **transaction**, consider the number of transactions a digital commerce enterprise processes.

- BBC claimed in 2011, that **Amazon customers made 35 transactions per second**.

COMMERCE

- there needs to be **redundancy**, ensuring that if one system is compromised another is available.

- **diversity** of systems is important as well, ensuring that the vulnerability of one system is not necessarily present in another.

- systems must remain unchanged, unless changed through a managed process, **integrity** is key to confidence in the transaction.

- **non-repudiation** is crucial to ensure the buyer has accountability for their actions.

How do we meet the security objectives?

COMMERCE

MOBILE DEVICES

- mobile devices are important to enterprises as they afford powerful devices with relatively straight-forward interfaces.

- constant connectivity is blurring the lines of when business activity occurs.

- challenging because consumers dictate mobile devices and enterprises need to accommodate employee choice.

- difficult for an enterprise to met security objectives on devices it does not fully control.

MOBILE DEVICES

- need to ensure employee is the only when in **possession** of a specific number.

- **reliable** transmission are crucial, as the wrong transmission can not enter the wrong hands.

- mobile devices are essentially computers, characterised by **connectivity**.

- data must be kept **confidential**, not only during transmission but storage as well as consumption.

INDUSTRIAL CONTROL SYSTEMS (ICS)

- industrial infrastructure that support many different types of businesses worldwide.
- communication is a crucial part of industrial control systems with many industrial networks.
- can comprise Human-Machine Interface (HMIs), Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCSs), Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), supervisory systems as well as telemetry systems.
- reliability and safety are the key concerns with considering industrial control systems (consequently, even many non-malicious threats can have severe consequences).

INDUSTRIAL CONTROL SYSTEMS (ICS)

- industrial control systems are not new, for many enterprises they are potentially very old.
- vulnerabilities may exist in workstations, that may utilise older versions of Microsoft Windows.
- generally, such systems do not rely on off-the-shelf consumer software.
- bespoke software that focuses on aspects such energy will typically be used on such systems.

INDUSTRIAL CONTROL SYSTEMS (ICS)

- industrial control systems can suffer from the same traditional threats as traditional information systems, due to use of some consumer systems.

- industrial control systems can also suffer from distinct threats and have different requirements (e.g. environmental and repair windows).

- ICSs are diverse, presenting a very big challenge to state and industry.

- Overlapping and confusing acronyms, confuse not only computing scientists but engineers in industry (e.g. an engineer may not know how to secure a consumer workstation).

COMMUNICATION

FLOW OF COMMUNICATION

- recall, cyber security is the concern of **all** stakeholders within an organisation, not a single person or entity.

- recall, complexity of systems and consider the flow of information within the enterprise.

- management **top-down** communication focuses on cyber security direction and objectives to key-decision makers.

- **lateral** and **bottom-up** communication focuses communications focuses on the human and technical cyber security specifics.

INTERNAL COMMUNICATION

- consider the communication to the **actors within the enterprise**.
- aim is to effectively communicate the **cyber security objectives** within the **context** of the enterprise.
- **assets** of the enterprise, the things the organisation cares about and why do they care about them.
- responsibilities and accountability for decision pertaining to considered risks.

EXTERNAL COMMUNICATION

- need to ensure external parties understand the **context** of the enterprise.

- clear communication of **assets**, what is perceived to be important to the organisation.

- if external entity is providing security what is the expectation and agreement.

- enterprise must understand what success looks like when external party is providing security.

STRUCTURE

- policy will be informed by consideration of assessment of cyber risk to assets.

- should be informed and communicate clear objectives as well as indicate responsibilities.

- may be many different instruments and approaches to assessing such risk, but this may not be the best communication structure.

- policy may be supported with additional explanation as well as information about the reason for controversy.

LANGUAGE

- language should simple and **clear** and **embrace the domain language** and specifics.

- directives should be **short** and **simple** as if it is too long people may ignore it.

- policies may be **inclusive** or **exclusive**, decisions need to be taken to determine the best option.

- inclusive policies indicate what is **permitted**, while exclusive policies state what is **prohibited**.

INCLUSIVE VS EXCLUSIVE

- inclusive policies do not need to be updated for every release of software or new application.

- exclusive policies could potentially need to be reviewed and revisited with a new application.

- consider the policy and the approach, targeting a single application is unrealistic if a policy has to be produced for every application.

EXPECTATIONS

- directives should not prohibitive what can not be prevented.
- directives can not be designed that makes them difficult or unrealistic to follow.
- directives should be realistic in the expectation of what they want in terms of desired behaviours.
- directives should be reasonable and within the legal and regulatory environment.

CATALOGUE

CATALOGUE

- much like metrics, there are large catalogues of directives that enterprise can consider and utilise.

- companies can purchase policies or incorporate established policies.

- catalogues usually comprises of detail lists to explain the motivation for them.

- arguments for the strengths and negatives for each directive also useful in management comprehending impact of policy.

LISTS

DIRECTIVE	DESCRIPTION	REASONING

LISTS

DIRECTIVE	DESCRIPTION	REASONING
Actual directive itself.	The motivation for the use of the directive in cyber security.	Several points that may motivate the inclusion of a directive or the exclusion of a directive.

LISTS

DIRECTIVE	DESCRIPTION	REASONING
Employees may only send emails on behalf of the enterprise on supported email services.	The motivation for this directive is to ensure that employees only use permitted email services when conducting business and not personal services, e.g. gmail.	This ensures that communications are under the purview of the organisation.
		The concern is that important business opportunities may be missed if individuals cannot access services.
Employees may use delivery and read receipts to provide proof of communication.	Regulatory as well as specific contracts requires proof of delivery and notification.	The technological implementation may make this difficult to actual provide and properly support.
		Reduces costs associated with proof of delivery for various domains.

LISTS

DIRECTIVE	DESCRIPTION	REASONING

VERIFICATION AND VALIDATION

VERIFICATION AND VALIDATION

- can construct **metrics** to determine that whether or not security objectives are being met.

- security solutions can be put in place to tackle know threats.

- verifications metrics confirm that solutions are meeting known requirements.

- this does not mean that security objectives of the enterprise are being met.

VERIFICATION AND VALIDATION

- evidence needs to be presented to **validate** that security objectives are being met.
- need more than just the latest known attacks are being defended against.
- need to ensure the system is resilient even against unknown threats.
- consequently, need to consider approaches that demonstrate it is reliable, redundant, maintains integrity and still maintain non-repudiation.

VERIFICATION AND VALIDATION

- verification can be complex, while analysis may state requirements are being met, difficult to confirm with the number of actors.

- network provider (both in terms of external wifi and mobile network), device manufacturer, software provider, application, environment provider, external applications etc.

- validation is complex due to the number of partners and the balance between personal and enterprise data.

- confidential is difficult to confirm, because of the lack of certainty that the device is in the correct hands.

VERIFICATION AND VALIDATION

- confidentiality is also difficult because individuals to continue use it while it being in the hands of others.

- can attempt to understanding by ensuring data is stored and transmitted in a secure fashion.

- control may be possible, but difficult to actually implement as individual use their devices in many ways.

- gather evidence to verify and validate security objectives on mobile devices is challenging, but this does not mean such test should be pushed.

PROBLEMS WITH POLICY

POLICY PROBLEMS

- many policies could lead to confusion, lack of clarity and may end up causing more harm than good.

- policies may curb and impact on business objectives, that could interfere with the success of the system.

- focus of policies is often on cyber risk rather than how people make decisions and what motivates them.