UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UTeM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 11

By

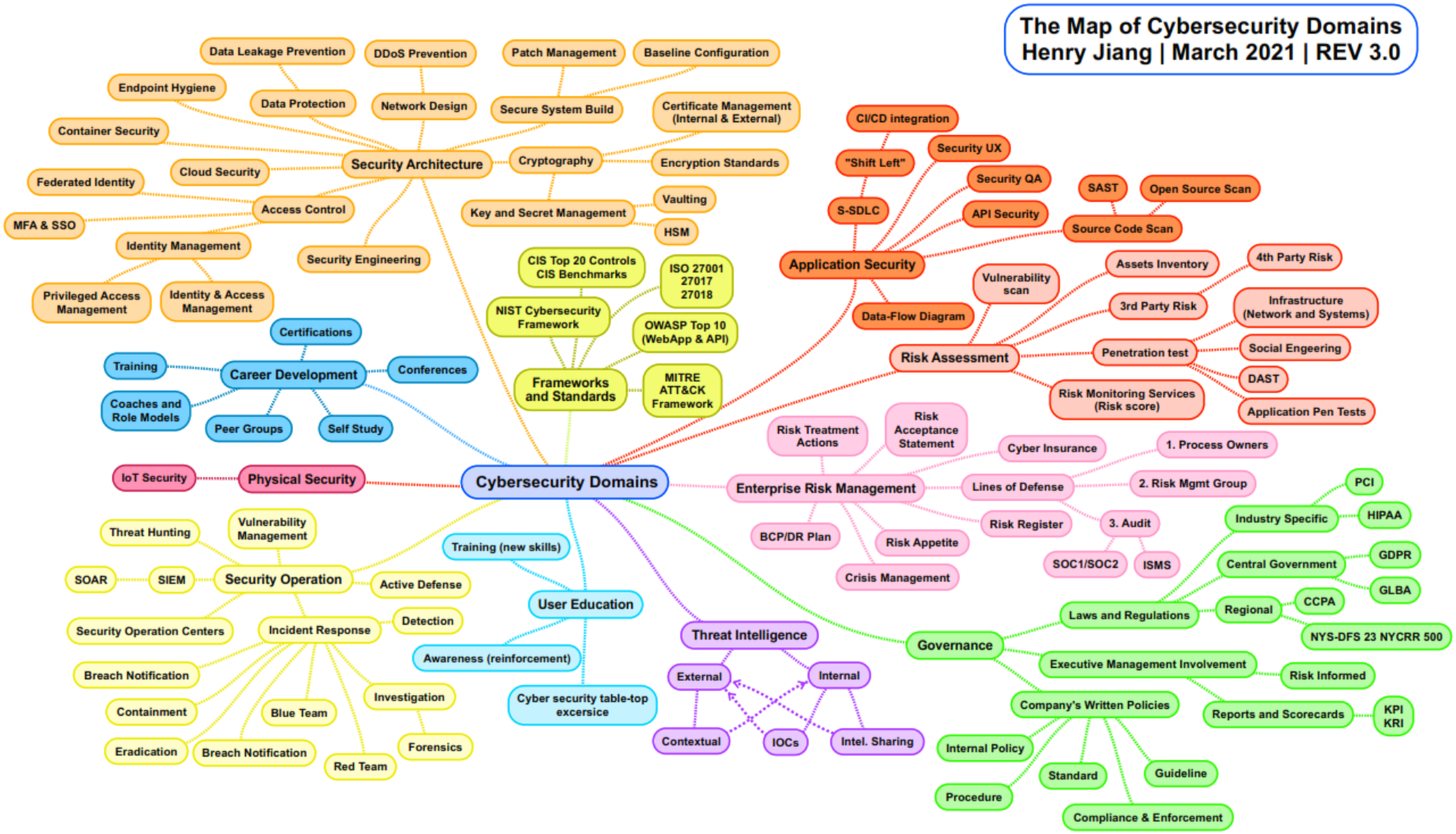
Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

Strategic Security Policy

Topics covered:

- Governance
- Guiding principles
- Corporate culture
- Policy
- Successful Policy Characteristics
- The Role of Government and industry


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Certificate Management (Internal & External)
Container Security
Cloud Security
Cryptography
Encryption Standards
Federated Identity
Access Control
Key and Secret Management
Vaulting
HSM
MFA & SSO
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Application Security
CI/CD integration
"Shift Left"
Security UX
S-SDLC
Security QA
API Security
SAST
Open Source Scan
Source Code Scan
Data-Flow Diagram
Vulnerability scan
Risk Assessment
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engeering
DAST
Application Pen Tests
Risk Monitoring Services (Risk score)
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Physical Security
IoT Security
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR Plan
Risk Appetite
SOC1/SOC2
ISMS
Crisis Management
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Training (new skills)
User Education
Security Operation Centers
Incident Response
Detection
Awareness (reinforcement)
Breach Notification
Containment
Eradication
Blue Team
Breach Notification
Red Team
Investigation
Forensics
Cyber security table-top excersice
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Company's Written Policies
Reports and Scorecards
KPI
KRI
Internal Policy
Standard
Guideline
Procedure
Compliance & Enforcement

Governance

- Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The Board of Directors is the authoritative policy making body.
- Executive management is tasked with providing support and resources. Endorsed by the Board of Directors and executive management, the CISO (or equivalent role) is vested with information security program management responsibility and accountability.
- The chain of command for the CISO should be devoid of conflict of interest. The CISO should have the authority to communicate directly with the Board of Directors.
- Discussion, debate, and thoughtful deliberation result in good decision making. Supporting the CISO should be an Information Security Steering Committee, whose members represent a cross-section of the organization. Typically, members represent a cross-section of business lines or departments, including operations, risk, compliance, marketing, audit, sales, HR, and legal.
- In addition to providing advice and counsel, their mission is to spread the gospel of security to their colleagues, coworkers, subordinates, and business partners.

Governance

In Practice

CISO Policy

Synopsis: To define the role of the CISO as well as the reporting structure and lines of communication.

Policy Statement:

- The COO will appoint the CISO.
- The CISO will report directly to the COO.
- At his or her discretion, the CISO may communicate directly with members of the Board of Directors.
- The CISO is responsible for managing the information security program, ensuring compliance with applicable regulations and contractual obligations, and working with business units to align information security requirements and business initiatives.
- The CISO will function as an internal consulting resource on information security issues.
- The CISO will chair the Information Security Steering Committee.
- The CISO will be a standing member of the Incident Response Team and the Continuity of Operations Team.
- Quarterly, the CISO will report to the executive management team on the overall status of the information security program. The report should discuss material matters, including such issues as risk assessment, risk management, control decisions, service provider arrangements, results of testing, security breaches or violations, and recommendations for policy changes.

In Practice

Information Security Steering Committee Policy

Synopsis: The Information Security Steering Committee (ISC) is tasked with supporting the information security program.

Policy Statement:

- The Information Security Steering Committee serves in an advisory capacity in regards to the implementation, support, and management of the information security program, alignment with business objectives, and compliance with all applicable state and federal laws and regulations.
- The Information Security Steering Committee provides an open forum to discuss business initiatives and security requirements. Security is expected to be given the same level of respect as other fundamental drivers and influencing elements of the business.
- Standing membership will include the CISO (Chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives. Adjunct committee members may include but are not limited to representatives of HR, training, and marketing.
- The Information Security Steering Committee will meet on a monthly basis.

Governance

- The steering committee serves in an advisory capacity with particular focus on the alignment of business and security objectives. Distributed throughout the organization are a variety of roles that have information security–related responsibilities. Most notably, data owners are responsible for defining protection requirements, data custodians are responsible for managing the protection mechanisms, and data users are expected to act in accordance with the organization's requirements and to be stewards of the information in their care.
- The Board of Directors (or organizational equivalent) is generally the authoritative policy-making body and responsible for overseeing the development, implementation, and maintenance of the information security program.
- The use of the term "oversee" is meant to convey the Board's conventional supervisory role, leaving day-to-day responsibilities to management. Executive management should be tasked with providing support and resources for proper program development, administration, and maintenance as well as ensuring strategic alignment with organizational objectives.

Governance

"*Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.*"

- Julie Allen, in her seminal work "Governing for Enterprise Security"

Governance

Organisational roles and responsibilities

- In addition to the CISO and the Information Security Steering Committee, distributed throughout the organization are a variety of roles that have information security–related responsibilities. For example:
  - **Compliance Officer**—Responsible for identifying all applicable information security–related statutory, regulatory, and contractual requirements.
  - **Privacy Officer**—Responsible for the handling and disclosure of data as it relates to state, federal, and international law and customs.
  - **Internal audit**—Responsible for measuring compliance with Board-approved policies and to ensure that controls are functioning as intended.
  - **Incident response team**—Responsible for responding to and managing security-related incidents.
  - **Data owners**—Responsible for defining protection requirements for the data based on classification, business need, legal, and regulatory requirements; reviewing the access controls; and monitoring and enforcing compliance with policies and standards.
  - **Data custodians**—Responsible for implementing, managing, and monitoring the protection mechanisms defined by data owners and notifying the appropriate party of any suspected or known policy violations or potential endangerments.
  - **Data users**—Are expected to act as agents of the security program by taking reasonable and prudent steps to protect the systems and data they have access to.
- Each of these responsibilities should be documented in policies, job descriptions, or employee manuals.

Governance

Governance of Enterprise Security

- Information security is not an end unto itself. Information security is a business discipline that exists to support business objectives, add value, and maintain compliance with externally imposed requirements. This type of relationship is known as strategic alignment.
- Organizational commitment to information security practices should be codified in a written policy. The information security policy is an authoritative document that informs decision making and practices.
- As such, it should be authorized by the Board of Directors or equivalent body. Derivative documents for specific audiences should be published and distributed. This includes an Acceptable Use Policy and Agreement for users, a thirdparty version for vendors and service providers, and a synopsis for business partners and clients.
- Three factors influence information security decision making and policy development: guiding principles, regulatory requirements, and risks related to achieving their business objectives.

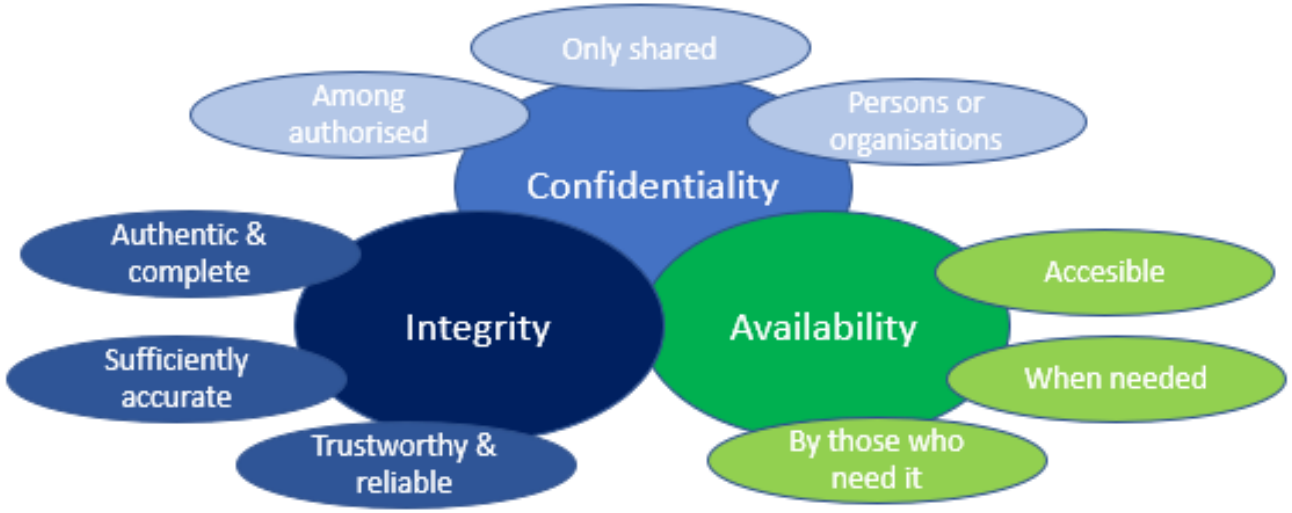
Guiding principle

- Over-arching statements that convey the philosophy, direction or belief of an organization.
- Guiding principles synthesize the fundamental philosophy or beliefs of an organization and reflect the kind of company that an organization seeks to be.
- Guiding principles serve to "guide" people in making the right decisions for the organization.
  - What policies and standards are needed?
  - What technologies are needed?
  - How architecture should be accomplished?
- Guiding principals are NOT policies but serve as guidelines in the formulation of thoughtful and comprehensive security policies and practices.

Guiding principle (cont...)

- They serve to "guide" people in making the right decisions (such a technology purchases or architecture direction).
- They can also serve as a guide-post on what policies and standards will be needed by an organization.
- Guiding principles provide a strong foundation for any organization.
- They can be specific to a certain function (e.g. Corporate Security) or more general such as IT Guiding Principles.
- Guiding principles set the tone for a corporate culture.

Highest Level Security Guiding Principles



- Every security organization should be concerned about the confidentiality, integrity, and availability of their key information assets and resources.
- This should be reflected in one or more of their key security guiding principals.

Sample Security Guiding Principles

- Everyone is responsible for security.
- All users and entities are authenticated.
- Principle of "least access" is appropriately applied.
- Risk exposure is balanced with the cost of risk mitigation.
- Security measures are proactively implemented.
- We will promote information classification, awareness and governance.

Sample Security Guiding Principles (cont…)

- We will use comprehensive architectural planning to ensure that all elements of the information security program are defined and planned.
- We will carefully balance the business need to quickly offer new products and services against the security risks it might pose to our customers or damage to our company brand or reputation.
- We will invest in information security at or above industry benchmarks for our business.

Sample Security Guiding Principles (cont…)

- We will adopt security industry standards where appropriate.
- We will evolve the practice of information security with our external and internal customers (best practice sharing on standards, solutions architecture, technology, processes and policies).

Corporate culture

- Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company, corporation, or institution.
- Corporate cultures are often classified by how corporations treat their employees and their customers.
- The three classifications are negative, neutral, and positive.
- A negative classification is indicative of a hostile, dangerous, or demeaning environment. Workers do not feel comfortable and may not be safe; customers are not valued and may even be cheated.
- A neutral classification means that the business neither supports nor hinders its employees; customers generally get what they pay for.
- A positive classification is awarded to businesses that strive to create and sustain a welcoming workplace, truly value the customer relationship, partner with their suppliers, and are responsible members of their community.

Corporate culture

- Let's consider a tale of two companies. Both companies experience a data breach that exposes customer information; both companies call in experts to help determine what happened.
- In both cases, the investigators determine that the data-protection safeguards were inadequate and that employees were not properly monitoring the systems. The difference between these two companies is how they respond and learn from the incident.
- Company A is quick to respond by blaming the department management, firing key employees, and looking for ways to avoid legally required customer notification.
- Company B leadership shares the report with the department, solicits internal and external feedback on how to improve, researches new controls, methodically implements enhancements, and informs customers in a timely manner so they can take steps to protect themselves.

Corporate culture

- A positive corporate culture that focuses on protecting internal and customer information, solicits input, engages in proactive education, and allocates resources appropriately makes a strong statement that employees and customers are valued. In these organizations, policy is viewed as an investment and a competitive differentiator for attracting quality employees and customers.

Policy

- A formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area.
- The role of policy is to codify guiding principles, shape behavior, provide guidance to those who are tasked with making present and future decisions, and serve as an implementation roadmap.
- For example, an information security policy is a directive that defines how the organization is going to protect its information assets* and information systems, ensure compliance with legal and regulatory requirements, and maintain an environment that supports the guiding principles.

Policy

- The objective of an information security policy and corresponding program is to protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information, protect the integrity of the information, and ensure the availability of information systems.

*Information asset

- Information is data with context or meaning. An asset is a resource with value. As a series of digits, the string 345934353 has no discernible value. Information asset is the term applied to the information that an organization uses to conduct its business.
- Examples include customer data, employee records, financial documents, business plans, intellectual property, IT information, reputation, and brand.
- Information assets may be protected by law or regulation (for example, patient medical history), considered internally confidential (for example, employee reviews and compensation plans), or even publicly available (for example, website content). Information assets are generally stored in digital or print format; however, it is possible to extend our definition to institutional knowledge.

Successful Policy Characteristics

- Successful policies establish what must be done and why it must be done, but not how to do it.
- Good policy has the following seven characteristics:
  1. Endorsed: The policy has the support of management.
  2. Relevant: The policy is applicable to the organization.
  3. Realistic: The policy make sense.
  4. Attainable: The policy can be successfully implemented.
  5. Adaptable: The policy can accommodate change.
  6. Enforceable: The policy is statutory.
  7. Inclusive: The policy scope includes all relevant parties.

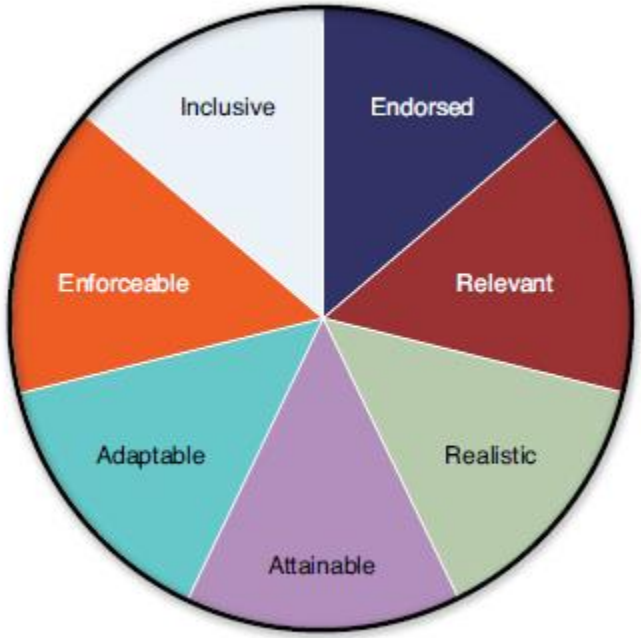


FIGURE 1.1 The policy pie.

Successful Policy Characteristics

Endorsed

- In order for an information security policy to be successful, leadership must not only believe in the policy, they must also act accordingly by demonstrating an active commitment to the policy by serving as role models. This requires visible participation and action, ongoing communication and championing, investment, and prioritization.

Relevant

- Strategically, the information security policy must support the guiding principles and goals of the organization. Tactically, it must be relevant to those who must comply. Introducing a policy to a group of people who find nothing recognizable in relation to their everyday experience is a recipe for disaster.

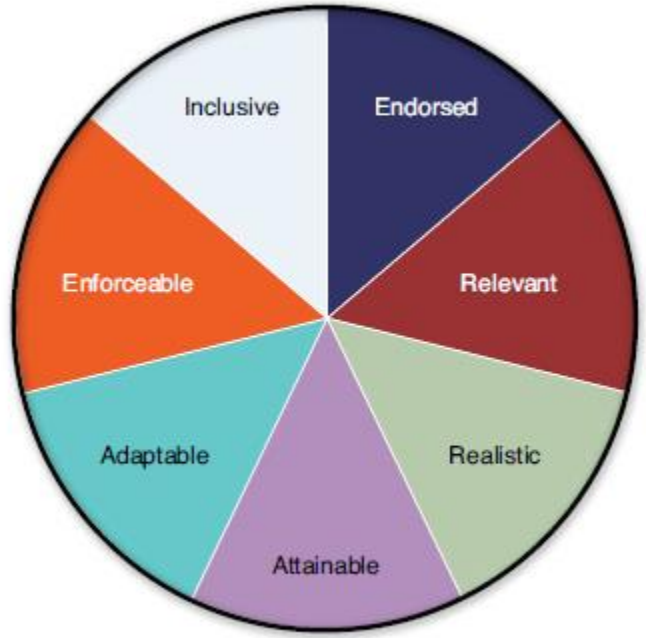


FIGURE 1.1 The policy pie.

Successful Policy Characteristics

Realistic

- Policies will be rejected if they are not realistic. Policies must reflect the reality of the environment in which they will be implemented.

Attainable

- Policies should only require what is possible. If we assume that the objective of a policy is to advance the organization's guiding principles, one can also assume that a positive outcome is desired. A policy should never set up constituents for failure; rather, it should provide a clear path for success.

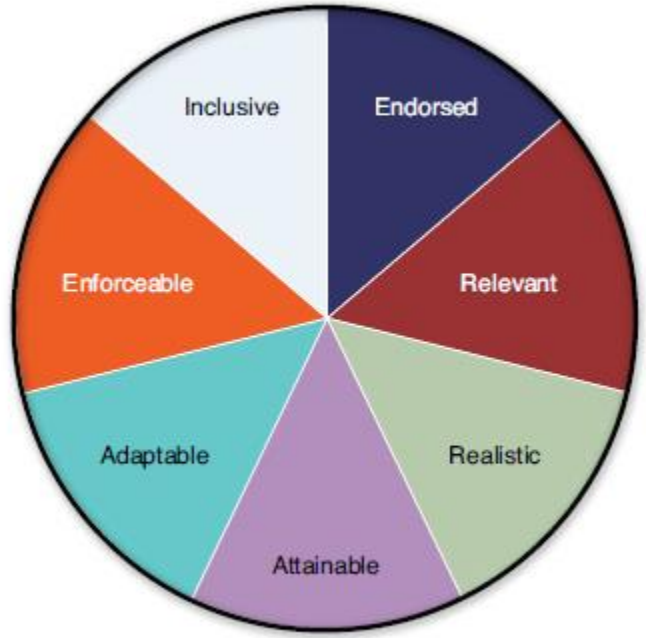


FIGURE 1.1 The policy pie.

Successful Policy Characteristics

Adaptable

- In order to thrive and grow, businesses must be open to changes in the market and willing to take measured risks. A static set-in-stone information security policy is detrimental to innovation. Innovators are hesitant to talk with security, compliance, or risk departments for fear that their ideas will immediately be discounted as contrary to policy or regulatory requirement. “Going around” security is understood as the way to get things done. The unfortunate result is the introduction of products or services that may put the organization at risk.

Enforceable

- Enforceable means that administrative, physical, or technical controls can be put in place to support the policy, that compliance can be measured and, if necessary, appropriate sanctions applied.

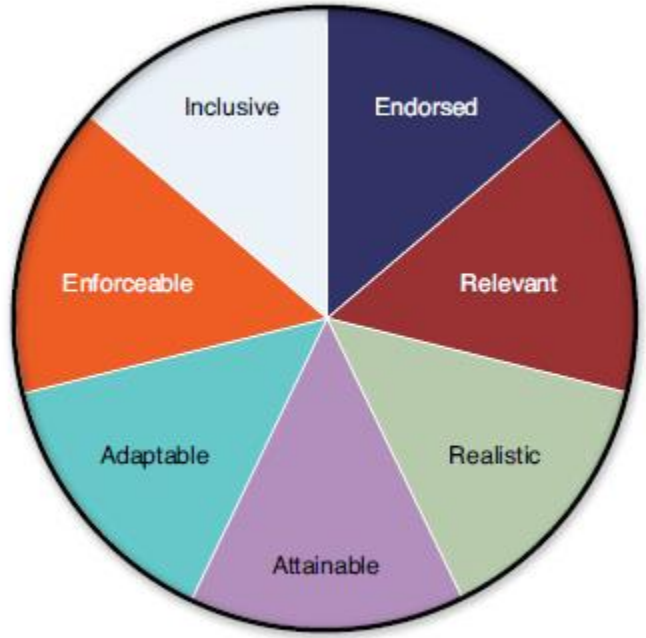


FIGURE 1.1 The policy pie.

Successful Policy Characteristics

Inclusive

- It is important to include external parties in our policy thought process. It used to be that organizations only had to be concerned about information and systems housed within their walls. That is no longer the case. Data (and the systems that store, transmit, and process it) are now widely and globally distributed.
- The trend toward outsourcing and subcontracting requires that policies be designed in such a way to incorporate third parties. Information security policies must also consider external threats such as unauthorized access, vulnerability exploits, intellectual property theft, denial of service attacks, and hacktivism.
- An information security policy must take into account organizational objectives; international law; the cultural norms of its employees, business partners, suppliers, and customers; environmental impact and global cyber threats. The hallmark of a great information security policy is that it positively affects the organization, its shareholders, employees, and customers, as well as the global community.

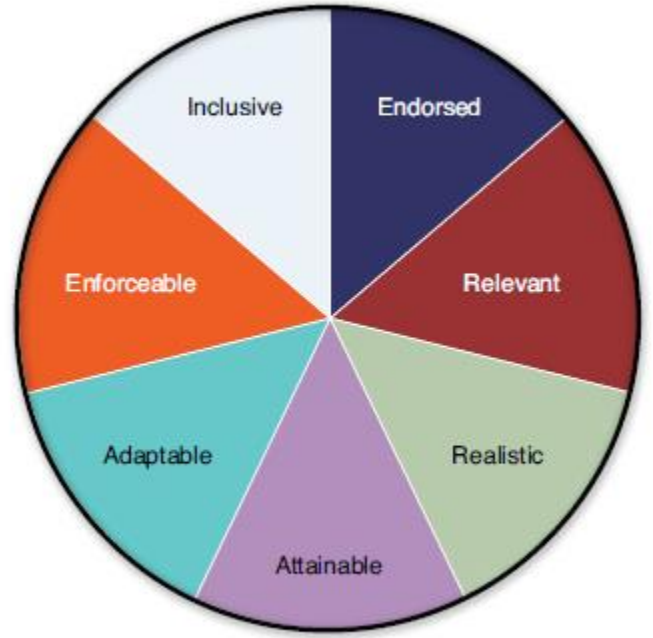


FIGURE 1.1 The policy pie.

The role of government

- At times, government intervention is required in order to protect its critical infrastructure and its citizens.
- Intervention with the purpose of either restraining or causing a specific set of uniform actions is known as regulation*.

Example of US government role

- In the 1990s, two groundbreaking pieces of information security–related federal legislation were introduced with the objective of protecting personal financial and medical records:
    - The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, Safeguards Rule
    - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

*https://www.differencebetween.com/difference-between-law-and-vs-regulation/

The role of government

Gramm-Leach-Bliley Act (GLBA)

- The purpose of the Act was to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. The Act permitted banks to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities. Lawmakers were concerned that these activities would lead to an aggregation of customer financial information and significantly increase the risk of identity theft and fraud.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- HIPAA Security Rule established a national standard to protect individuals' electronic personal health information (known as ePHI) that is created, received, used, or maintained by a covered entity, which includes healthcare providers and business associates.
- The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Covered entities are required to publish comprehensive information security policies that communicate in detail how information is protected.

The role of government

Example of European Union role

- European nations recognize and value privacy as a basic human right. Together, they had devise and introduced the General Data Protection Regulation (GDPR).

General Data Protection Regulation (GDPR)

- The European Union's (E.U.) General Data Protection Regulation (GDPR) is a revolutionary and comprehensive data privacy law. The GDPR, which was approved in 2016 and came into force in May 2018, sets limits on the collection and use of personal data belonging to an E.U. data subject.
- The law also grants significant rights to E.U. data subjects. One of the most famous rights is the right to be forgotten. Under this provision, data subjects can request that organizations permanently delete the data subject's personal information.

The role of government

Example of Malaysian government role

- Malaysia also recognizes data privacy through the enactment of the Personal Data Protection Act 2010.

Personal Data Protection Act 2010

- This act regulates the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.
- Refer to previous lecture on PDPA 2010 for more details.

The role of industry

Example of industry role

- The PCI Council is not a government agency; rather, it is a private industry organization. The PCI Council, formed in 2006, creates safeguards designed to protect credit card data.

Payment Card Industry (PCI) Data Security Standard (DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council.
- The DSS offers a single approach to safeguarding sensitive cardholder data for all credit card issuers. It identifies 12 basic categories of security requirements that must be followed to protect credit card data.
- All merchants who accept credit cards must comply with the PCI DSS. PCI has different compliance requirements for different merchants that are based upon the size of the merchant's credit card operations.
- Any merchant that accepts credit cards must comply with the DSS. This means that they must implement and follow the DSS rules. The credit card brands enforce DSS compliance. Most of the credit card brands also require merchants to validate their compliance with the rules.

Thank You

MyUTeM

www.utem.edu.my