Cyber Security

Jhuma Dutta

Presented By
Prof. Jhuma Dutta
Department of Computer Science and Engineering
Jalpaiguri Government Engineering College

jhuma.dutta@cse.jgec.ac.in

April 22, 2022

Overview I

1. Introduction
2. Motivation
3. Challenges
4. Objectives
5. Cyber Security Policy

Introduction

- **Cyber/Cyspace:** Relating or Characteristics of the culture of computers, IT, virtual world using ICT tools and Networks
- **Cyber Security/Computer Security/IT Security:** Protection of computer systems and network from information disclosure, theft or damage to their hardware, software, electronic data as well as from the disruption or misdirection of the services they provide

Motivation

The field is becoming increasingly significant due to continuous uses of computer systems, the internet, wireless network and due to growth of Smart Devices including smart phones

Challenges

Vulnerabilities

A Vulnerability is the weakness in design, implementation, operation or internal control

Attacks

- Backdoor: is any secret method of bypassing normal authentication or security controls
- Denial-of-Service(DoS):are designed to make a machine or network resources unavailable to its intended users
- Direct access Atack: an unauthorised user gaining physical access to a computer is most likely able to directly copy data from it
- Eavesdropping: secretly listen to a conversation between hosts on a network
- Phishing Attack: is a type of social engineering attack attempt to acquiring sensitive information like login credentials, credit card details
- Side Channel Attack:gather information from the program execution

Objectives

Cyber Security

- refers to the ability to control access to networked systems and the information they contain
- refers to methods of managing people, process, and technology to prevent, detect and recover/respond from damage to confidentiality, integrity and availability of information in cyber space

Objectives

Security Objectives:

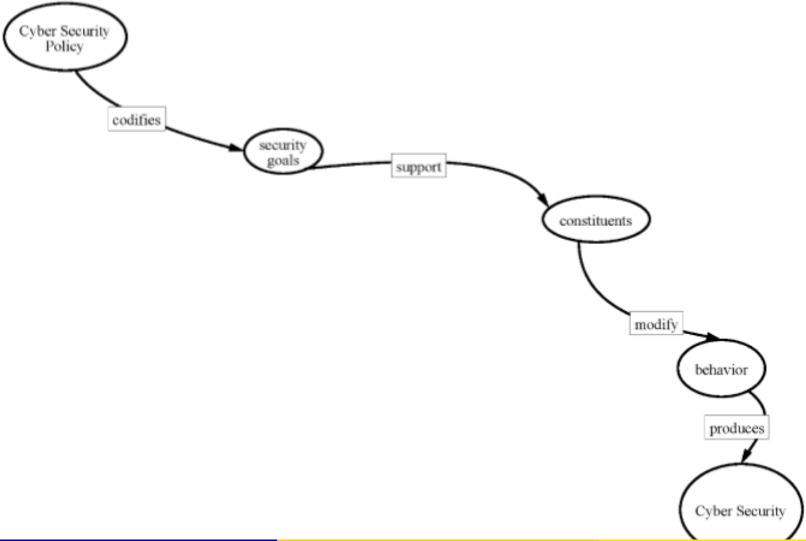
1. prevent, detect, respond(security goal)
2. people, process, technology(addresses methods common to both technology management in general and cyber security management as specialised field)
3. confidentiality, integrity and availability(security objective)

- **Confidentiality:** refers to keep information within authorised users
- **Integrity:** refers to maintain the authenticity, accuracy
- **Availability:** refers to the timely deliver of functional capability

Cyber Security Policy

- Cyber has created productivity enhancements throughout society, effectively distributing information on time basis
- The policy is applied to a variety of situations that concern cyber security
- Policy refers to laws and regulations concerning information distribution, private enterprise objective for information protection, computer operation methods for controlling technology and configuration variables in electronic devices
- cyber security policy refers to directives designed to maintain cyber security

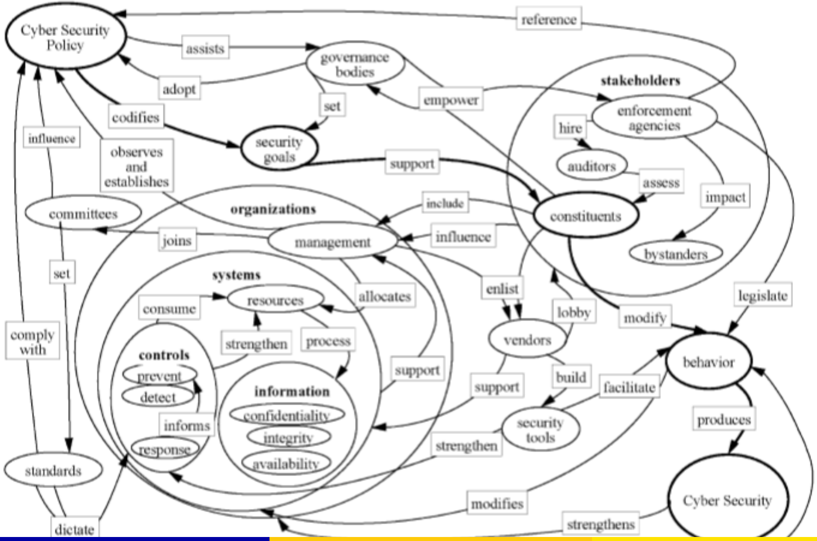
Cyber Security Policy



Definition

Cyber Security Policy is presented as something that codifies the security goals in support of constituents who are expected to modify their behaviour in compliance with the policy to produce cyber security

Cyber security Policy Perspective



Cyber Security Policy Perspective

- The figure flashes out the concept, adding the color of different perspectives of cyber security policy.
- The links to and from the "governance bodies node" illustrates that cyber security is adopted by governing bodies as a method of achieving security goals.
- enforcement agencies node establish the laws, rules and regulations that are meant not only to effect constituent behavior but also effects others, who thereby becomes stakeholders of the policy process.
- The links on the far left acknowledge the role of standards that are set by management of organizations who are bound by the governing bodies to comply with policy.

Cyber Security Policy Perspective

- The links emanating from the node labeled “vendors” depicts the vendor relationships of constituents and management, who both influence and are influenced by vendors who provide tools for security policy compliance and support systems security with products and services.
- “organizations” node refer to an organization that is subject to policy. It shows that such organizations observe cyber security policies issued by governing bodies as well as establish their own internal cyber security policies. It also illustrates that organizational management is both supporting and is being supported by systems that are impacted by security policy.
- The “systems” node refers to the systems used to operate cyberspace, highlighting the interdependent relationship between security controls and system resources.

Domains of Cyber Security Policy

cyber security policy is adopted by a governing body and formally applies only to the corresponding domain of governance. The constituents of cyber security policy, who may also be considered as stakeholders may very with the scope of the policy

e.g.

- nation-state policy will encompass all citizens and perhaps foreign businesses operating within its domain
- corporate cyber security policy will apply only to staff with which the cooperation has employment or other legal agreements which may reasonably be expected to motivate behavioral modification.

Goals of different Domains of Cyber Security Policy

- The content of security policy will change with the goals of the corresponding governing body.
- The goals of nation-state security are very different from the goals of corporate security, and so policy statements and corresponding expected activities in support of policy will appear very different.
- The way policy is compiled, documented by enforcement agencies, and ratified will also differ with its corresponding governing body and constituency.
- In government, the process by which goals are codified into policy and the process by which policies are codified into legislation are separate and distinct processes.
- However, in corporations, it is common to have one central security department responsible for both the cyber security policy and the associated standards and procedures which are the corporate equivalent of regulatory guidance.

Goals of different Domains of Cyber Security Policy

Where security is a priority for an organization, it is common to see cyber security policies issued by multiple internal departments with overlapping constituencies, who then sometimes detect policy incompatibility issues in trying to follow them all simultaneously.

Laws and Regulations

- nation-state cyber security policy is currently considered to be a subset of national security policy.
- Even if nation-state cyber security policy was considered to be on the same plane as foreign policy or economic policy, these policies do not have the same force as law.
- policies are established and articulated through reports and speeches, through talking points and negotiations.
- Policy is used to guide judgment on what laws and regulations to consider. It does not refer to the laws and regulations themselves.
- laws, and regulations would reflect a wise and thoughtfully conceived policy. nevertheless, it is possible to have cyber security executive directives, laws, and regulations without having articulated a cyber security policy at all.

Examples

- China has clearly established a policy that cyberspace activities critical to nation-state operations shall be controlled (Bishop 2010).
- This policy states clearly that the Internet shall serve the interests of the economy and the state.
- The policy has led to laws and regulations that allow the Chinese government to segregate, monitor, and control telecommunications facilities as well as block access to Internet sites they identify as contrary to their interests.

Examples

- In the united States, by contrast, most laws and regulations that impact cyber security were not developed specifically to address issues of cyberspace, but have emerged as relevant to cyber security in the context of policy enforcement.
- The policy is often economic in nature.
- A 2009 u.S. Cyber Security Policy Review actually redefined the word policy: "Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace
- and encompasses the full range of threat reduction, vulnerability reduction, prevention, international engagement, incident response, flexibility, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure"

Examples

- as they relate to the security and stability of the global information and communications infrastructure"
- This is the full range of issues to be considered when developing security policy. Moreover, the result of this review was not a policy recommendation. It simply outlined a strategy for ongoing communications and cooperation between the public and private sector with the goal of increasing national resilience to cyber attack
- Whether or not a government cyber security policy is articulated, its cyber security rules will be limited to the scope of its governance domain. That is, a branch or agency of a government will be within the scope of, and thus subject to, any government-wide regulation, so its own policy and rules must be consistent with that broader scope.

Laws for different agencies

- A branch or agency will only be able to create new legislation for its own constituency and within its own charter.
- For example, cyber security policy issued by an industry regulator will apply only to those industries in its regulatory domain
- An energy regulator will be able to require an energy facility to have redundant communications, but it will not be able to require that telecommunications providers lay redundant cables to each energy facility.
- Only a telecommunications industry regulator may set rules for the telecommunications industry, and the charter is not likely to include services provided to another regulator's domain.

Enterprise Policy

- Private sector organizations are generally not as constrained as governments in turning senior management policies into actionable rules
- In a corporate environment, it is typical that policies are expected to be followed upon threat of sanction, up to and including employment termination.
- For example, human resources, legal, or accounting policies have been codified to the point where any instance of noncompliance may amount to reason for termination.
- Where mid-level managers support processes such as staff hiring or expense filing, they may be expected to bring department activities into compliance with those policies, and often will have to establish department-level metrics for compliance

Enterprise policy

- As in case of Government, Such sub organization will be subject to constraints of authority in scope. Though there are exceptions in places that take information classification very seriously
- A corporation security policy issued by a Chief Executive Officer will generally apply to an entire corporation, but one issued by a Chief Information Officer will typically only apply to the technology staff.
- An unfortunate difference between most corporate cyber security policies and those issued by a legal or human resource department is that cyber security policies often leave the assessment of cyber security risks to mid-level managers who may not be familiar with cyber security or risk management concepts.

Enterprise Policy

- a cyber security policy may state, “where risk of information confidentiality compromise is high, the information should not be allowed to be shared with a vendor without a duly diligent review of vendor capability to secure information.” This type of policy leaves the information risk assessment to a manager who may be motivated to cut costs by outsourcing part of the department information flow.

Technology Operations

- To assist clients in complying with legal and regulatory information security requirements, the legal, accounting, and consulting professions have adopted standards for due diligence with respect to information security, and recommended that clients model processes around them.
- Where a standard becomes the preferred mode of operation for securing a technology environment, it will often be referred to as a cyber security policy for technology operations and management.
- These technology operations policies dictate simply that the standard should be followed, or they customize the standard with specific roles and responsibilities for process execution within the computer operations organization,

Technology Operations

- The scope of the policy will be limited to the management and operations of a well-defined technology platform
- The same organization will run multiple technology platforms, but their cyber security policy will apply only to a subset
- We will typically use the term policy to refer to higher level management directives that articulate and codify strategy for overall cyber security goal achievement as opposed to policy for the correct operation of a technology-only process.
- For example, the words "firewall policies" or "UNIX security policy" indicate that the object is a set of technical configuration variables rather than a directive by high-level management.

Technology Configuration

- Many technology operations standards are implemented using specialized security software and devices, technology operators often refer to the standard-specified technical configuration of these devices as “security policy.”
- These specifications have over the years been implemented by vendors and service providers, who devised technical configurations of computing devices that would allow system administrators to claim compliance with various standards.
- This has led vendors to label alternative technical configurations for their products as “security policies.” Vendor marketing literature presents these technical configurations as “policy” in an effort to align their solutions with the overall enter www

Strategy versus Policy

- Cyber security policy articulates the strategy for cyber security goal achievement and provides its constituents with direction for the appropriate use of cyber security measures.
- The direction may be dictated by a governance body.
- We also recognize that independent enterprises need to establish management directives in support of cyber security strategy, and we use the modified term, “enterprise policy” to refer to policies that apply only within a given enterprise community
- Such enterprise policy is often guided by standards for cyber security such as ISO, NIST those standards by themselves are not policies. Such standards typically contain a combination of process guidance with technology control recommendations. The process guidance recommends that policy be established, but cannot by itself properly be called policy.

Thank you

Questions?

jhumadutta81@gmail.com