
प्रणाम
vrkmPhoto

Information Systems Security

Pintu R Shah

Classroom Rules

- ✓Please Switch off your mobile phones or put it in a silent mode.
- ✓Maintain Discipline in the class.
- ✓No cross talk is allowed during the lecture.

Attendance

- It is expected that students will attend all classes. Attendance will be checked at the beginning of each class so make sure to be in on time; tardiness *disturbs everyone*. If you miss any classes, it is your responsibility to learn any missed material and then discuss your doubts with the faculty.
- Missing number of classes more than the percentage allowed by the institute regulations will result in a defaulter for the student.

Ask Question!

- I appreciate people asking questions during my lectures - it lets me know which concepts you are having difficulty with. Any question student asks is an important question regardless how he/she or others feels about it. Ask any question you think of directly or not directly pertinent to the lecture, I would be happy to entertain them during or/and at the end of the class.
- Sometimes I don't know the answer, but I'm happy to dig around and report back at the beginning of the next class.

- ***I've learned a lot over the years as a result of student questions!***

Frequency of Meeting

- 2 hrs of lecture per week
- 2 hrs of practical per week

Assessment

Sr. No.	Description	Marks
1	Term End Examination	100 Marks (Scaled down to 50)
2	Internal Continuous assessment	50 Marks
2.1	Class Test 1 and 2	20 Marks
2.2	Lab work	10 Marks
2.3	Assignment	10 Marks
2.4	Class Participation	10 Marks

Lab work and Assignments

- ✓Student will have to complete 10 experiments and one case study during the term.
- ✓Late submission will have 50% penalty.
- ✓Submit soft copy of your work with your name, class, roll no., SAP No. and date on MS Teams.

Important Note:

This subject will touch on sensitive issues including advance attack ideas, vulnerabilities and so forth

If a student is found to employ acquired knowledge with a purpose of launching an attack, he/she will be given a Fail grade and disciplinary action will follow.

Hacking Without Proper Approval is an offence and Punishment for same includes 3 yrs imprisonment or fine of Rs. 5,00,000 /- or Both

Course Policy

MS Team Code

savykmr

Syllabus

- Introduction
- Design Principles
- Cryptography
- Identity and Access Management
- Security Technologies
- Risk and Incident Management
- Legal and Ethical Issues

Let’s Start..

Remember

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu, The Art of War

Unit 1: Introduction

In this unit..

- Basic Components of Cybersecurity
- Vulnerabilities, threats , Attacks and Controls
- Goals of security
- Security System development life cycle
- NIST Cybersecurity Framework
- MITRE ATT&CK® Framework

Why Information Security?

Our love with Internet

" Criminal go where people go"

https://www.youtube.com/watch?v=7VgIayOpjEc

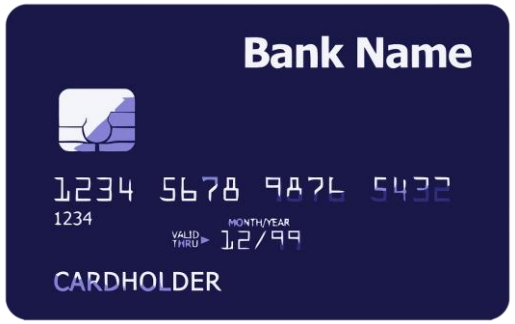

ASHLEY MADISON®
Life is Short. Have an Affair.®

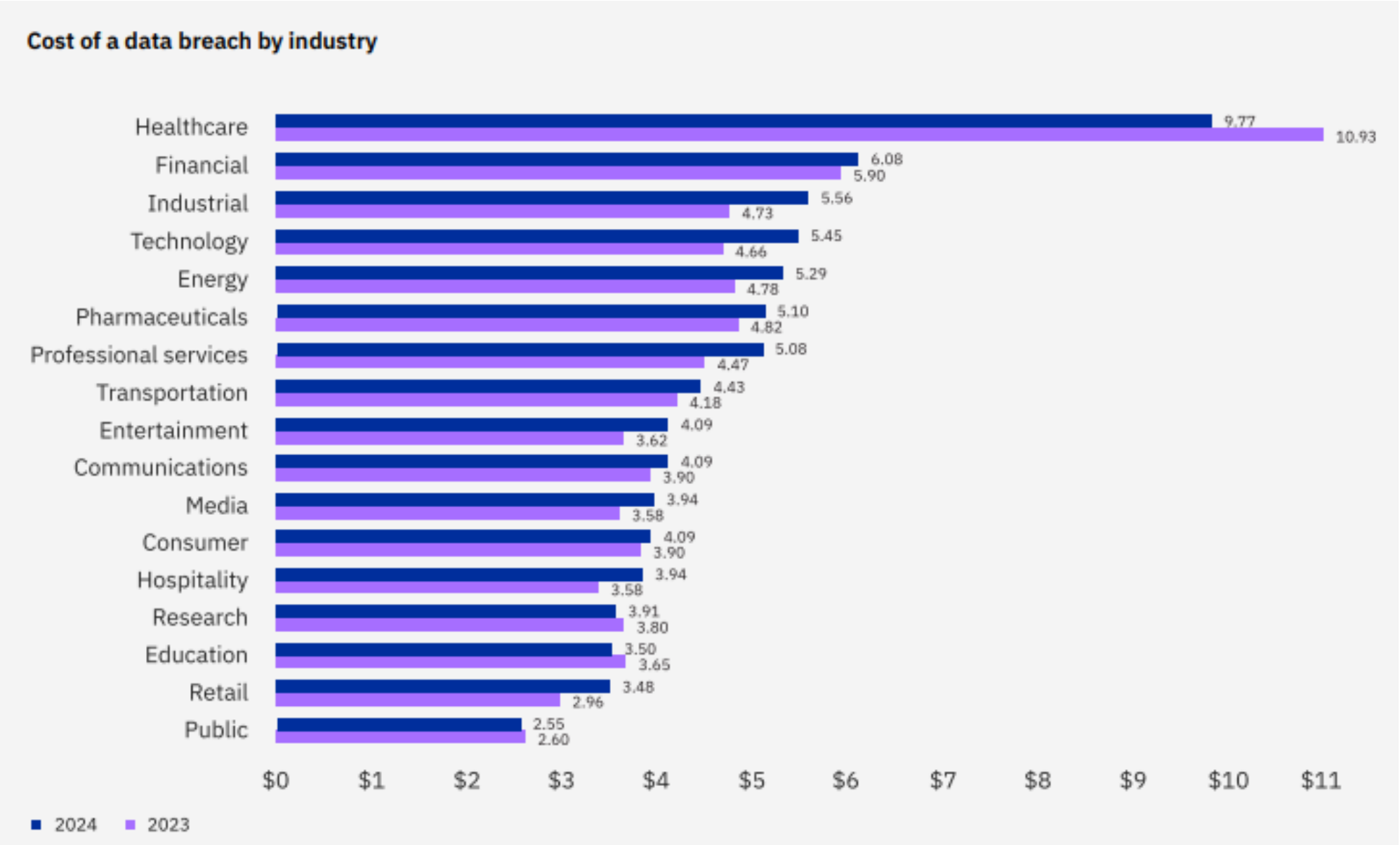

CapitalOne

But an attacker isn't interested in me…

Wrong!!! You are exactly what an attacker wants!

Spam	Harvesting	Privacy	Financial	Device control
• Phishing and malware • SNS spam	• Emails • Chats • Contacts • Company confidential information • Login credentials • Medical Data	• Messages • Call records • Photos • GPS coordinates	• Bank account details • Email account ransom	• Zombie • Installing malware/Adware for click bait revenue • Premium SMS • Crypto-mining





Measured in USD millions
Source: 2024 Cost of Data Breach Report- IBM

Cost of a data breach by country or region

#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	—
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Measured in USD millions
Source: 2024 Cost of Data Breach Report- IBM

Activity - 1

Organization	Data Breach Date	What was compromised?	Impact	Current Status
Medibank				
Optus				
Canva				
Microsoft				
Facebook				
Linked In				
JW Marriot				
Home Depot				
AIIMS Attack				
Cosmos Bank				

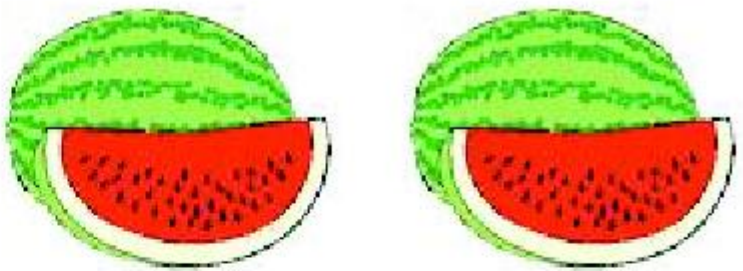
Types of records compromised

- Customer Personally Identifiable Information (PII)
- Anonymized customer data
- Intellectual Property
- Other sensitive information

NaMo on Cybersecurity

Security

- Asset(s)
- User(s)
- Adversary



Cyberspace

- A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (NIST SP 800-30 Rev. 1).
- “Cyberspace is a time-dependent set of interconnected information systems and the humans that interact with these systems”. (Ottis & Lorents, 2010)
- The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. (NISTIR 8074 Vol. 2)

Assets in Cyberspace

Information assets

- Information itself
- Information infrastructure (e.g. Internet, embedded software, firmware, communication protocols etc.)

Non-Information assets

- Physical entities connected on Internet:
  - Critical infrastructure: energy grid, water supply, public health, transportation, telecommunications, financial services, etc.
  - Internet of Things:
    - ✓ Connected and self-driving vehicles
    - ✓ Connected medical devices
    - ✓ Connected home automation and entertainment systems

Cybersecurity is protection of assets in cyberspace

Cybersecurity

- Cybersecurity is the collection of **tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance** and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected **computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information** in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

➢ Confidentiality

➢ Integrity, which may include authenticity and non-repudiation

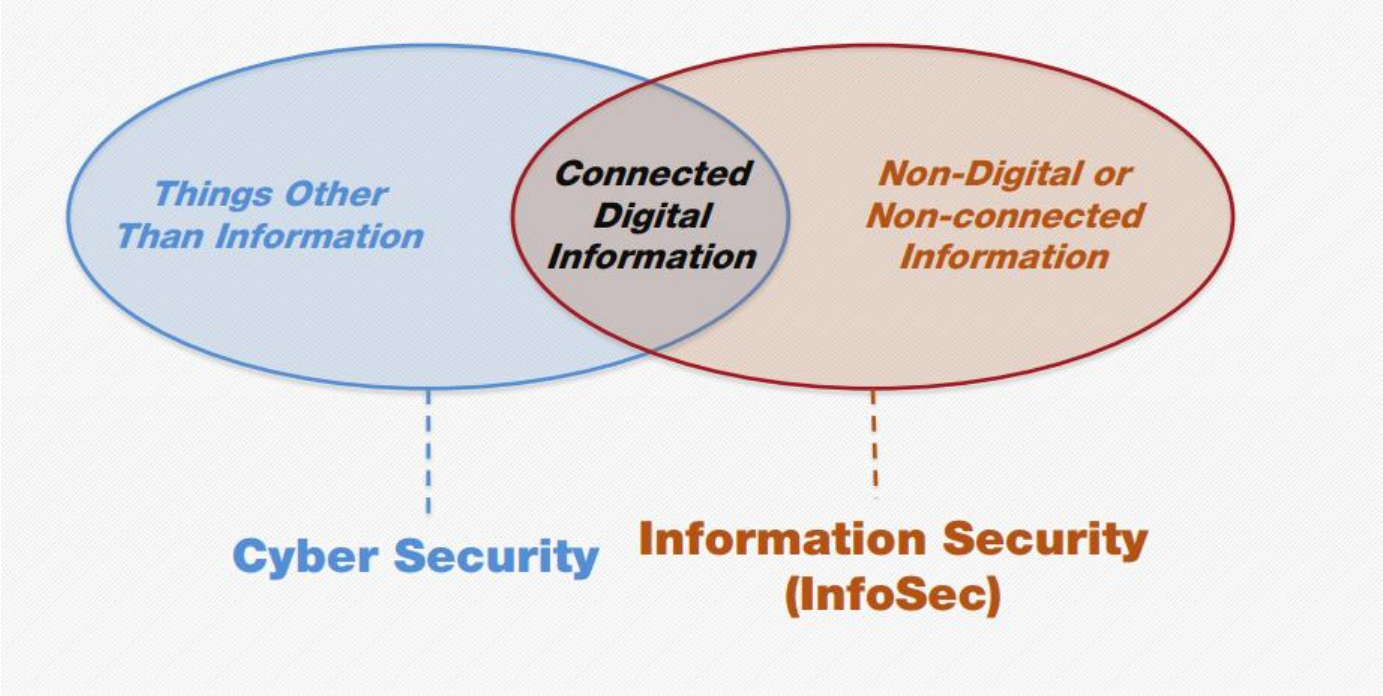
➢ Availability

- Source: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Cybersecurity

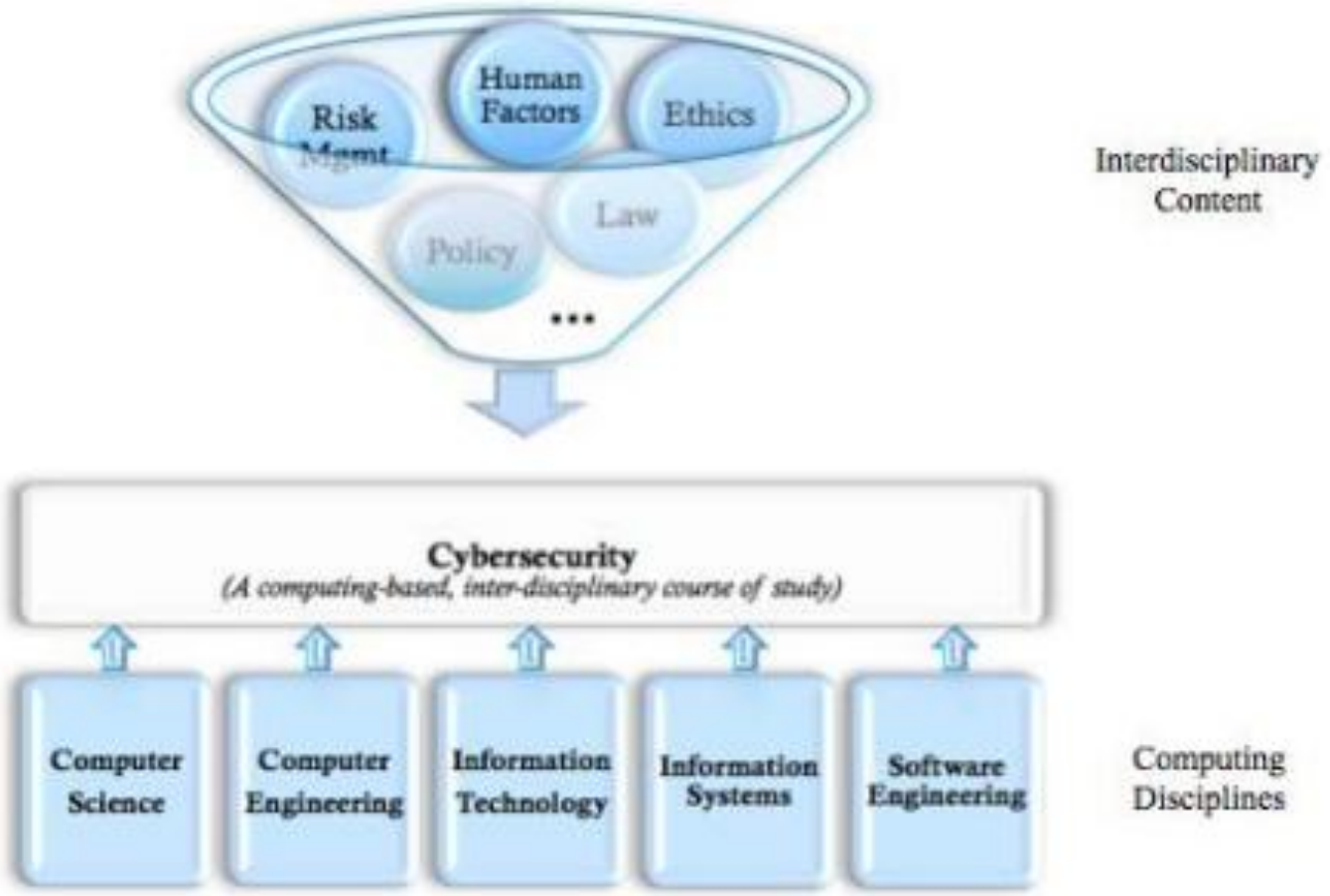
- A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management. (CSEC2017 JTF)

Cybersecurity v/s Information security

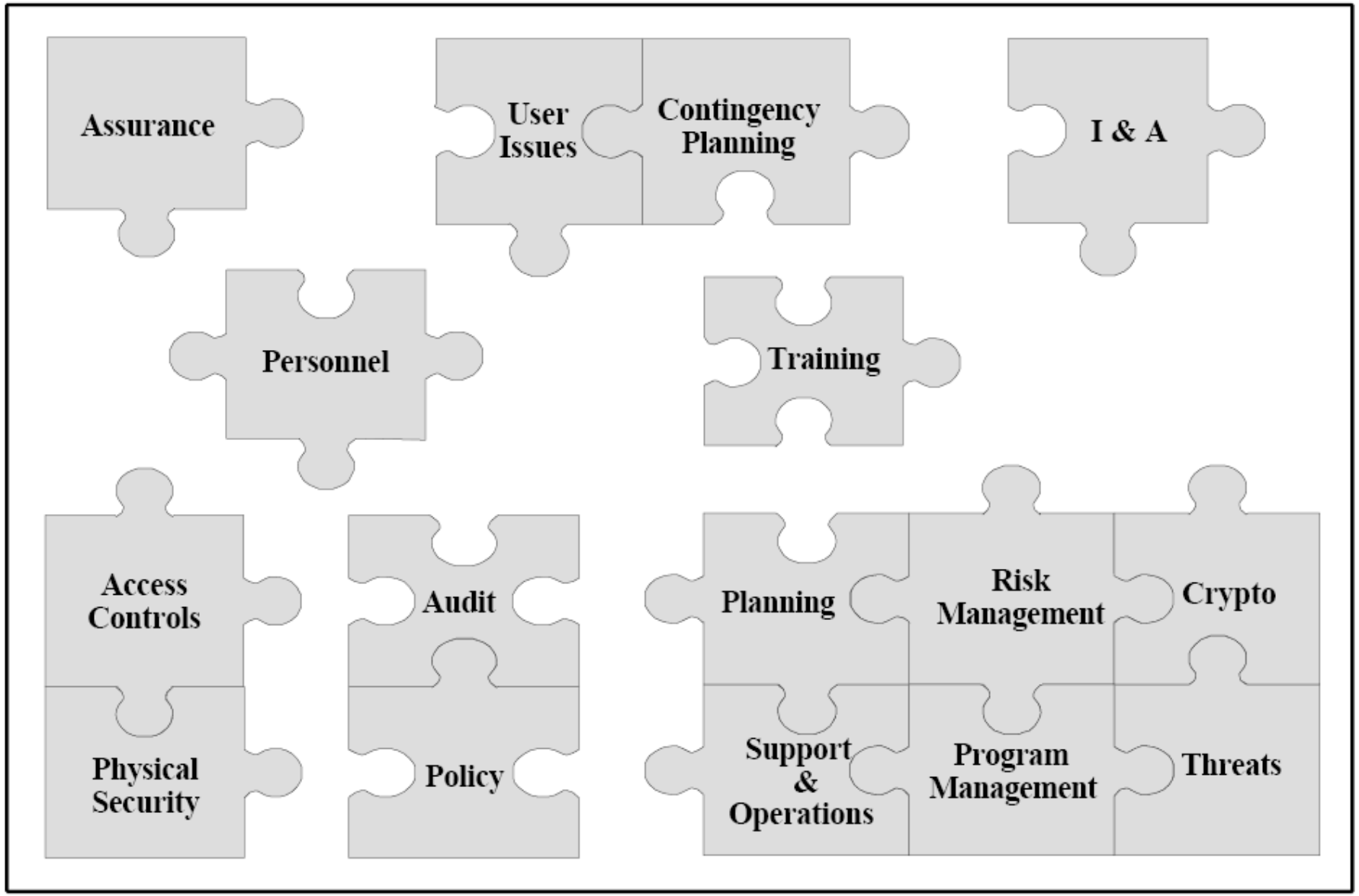


Elephant and six blind men

Structure of the cybersecurity discipline



https://www.cyberseek.org/index.html



Evolving trends

	1990s	2000s	2010s	2020s
Offenses	• Virus • Worms • Open Nets • Insecure configs	• Script Kiddies • Client-side attacks • Automated probes/scans • Too many alerts/logs	• APTs • DDoS • Botnet • Phishing • Ransomware	• Attacks causing Irreversible harm • New threats from/to AI systems
Defenses	✓Anti-Virus ✓firewalls ✓Security guidelines	✓ SEIM ✓ IDS ✓ Layered architecture	✓ Endpoint Detection and Response (EDR) ✓ Identity and Access Management (IAM)	✓ Artificial Intelligence ✓ Neural networks ✓ Blockchain
Age of	Protection →	Detection →	Response →	Cyber resilience

Activity 2

- Search for following
  - Loki Locker
  - Kaseya Ransomware
  - REvil Ransomware
  - Mirai malware attack
  - Silex Malware
  - Bashlite IoT Malware
  - Petya Ransomware

Critical Characteristics of Information

The value of information comes from the characteristics it possesses:

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

CIA triad

Confidentiality

- A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

- "Need to know" basis for data access
  - How do we know who needs what data?
    Approach: access control specifies *who* can access *what*
  - How do we know a user is the person he claims to be?
    Need his identity and need to verify this identity
    Approach: identification and authentication

- Confidentiality is:
  - difficult to ensure
  - easiest to assess in terms of success (binary in nature: Yes / No)

Integrity

- The property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

  - Integrity is more difficult to *measure* than confidentiality
    Not binary – degrees of integrity
    Context-dependent - means different things in different contexts

  Integrity of an item is preserved means item is:
  - Precise
  - Accurate
  - Unmodified
  - Modified only in acceptable ways
  - Modified only by authorized people/ processes
  - Consistent
  - Meaningful and usable

Integrity vs. Confidentiality

- Integrity is concerned with unauthorized *modification* of assets (= resources)
- Confidentiality is concered with *access* to assets

Availability

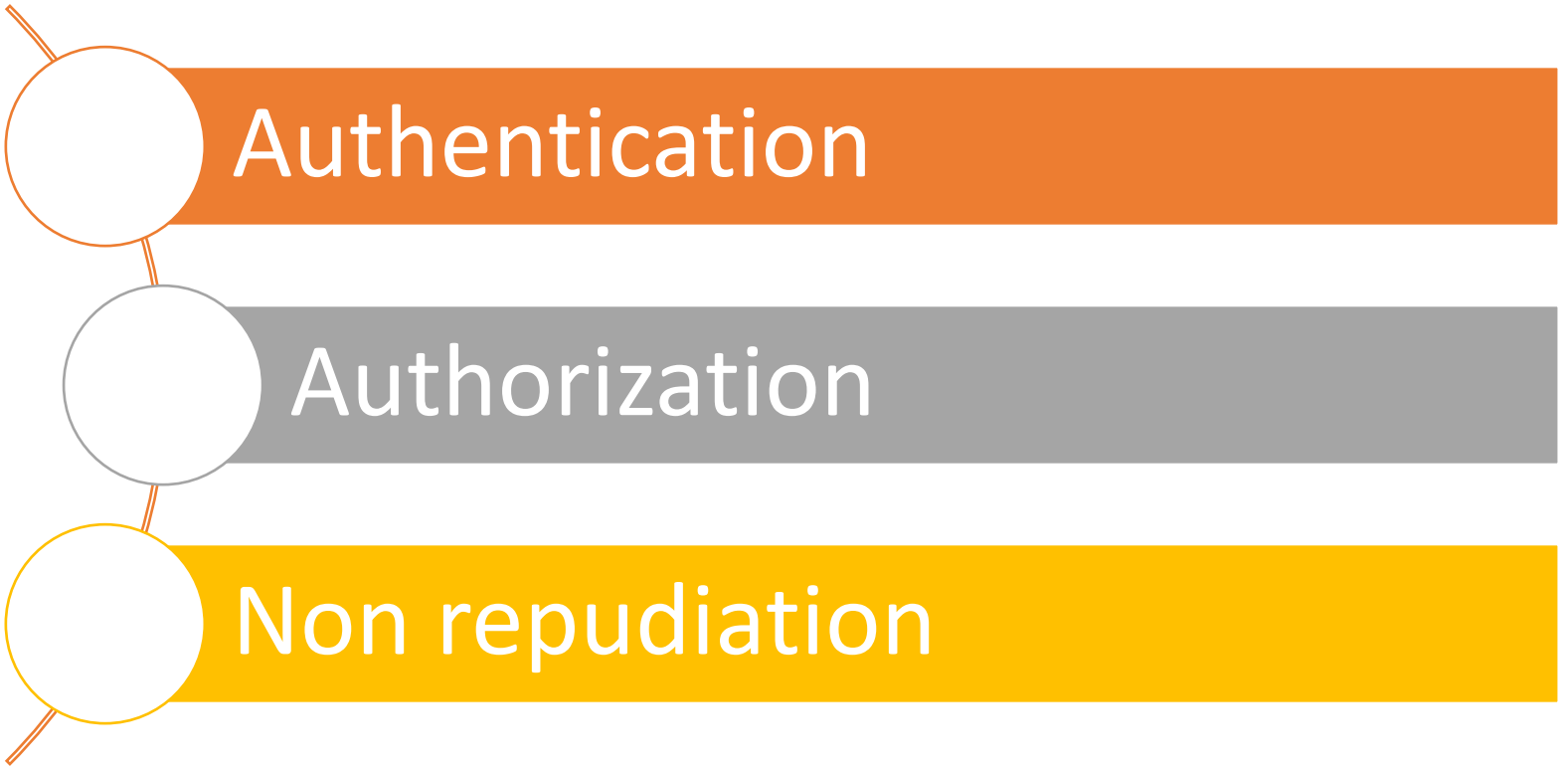
- The property of being accessible and usable upon demand.

- We can say that an asset (resource) is available if:
  - Timely request response
  - Fair allocation of resources (no starvation!)
  - Fault tolerant (no total breakdown)
  - Easy to use in the intended way
  - Provides controlled concurrency (concurrency control, deadlock control, ...)

Test your understanding

- https://forms.office.com/r/yULWJtXzgW

CIA or CIAAAN… ☺



Need to Balance CIA

- Example 1: C vs. I+A
  - Disconnect computer from Internet to increase confidentiality
  - Availability suffers, integrity suffers due to lost updates
- Example 2: I vs. C+A
  - Have extensive data checks by different people/systems to increase integrity
  - Confidentiality suffers as more people see data, availability suffers due to locks on data under verification)

Threat

- The threat is essentially the “who” or “what” that can do you harm if given an opportunity. They cannot do harm on their own.
- Malicious or Malignant
- Malignant threat are always present.
- Threats - examples
  - Viruses, trojan horses, etc.
  - Denial of Service
  - Stolen Customer Data
  - Modified Databases
  - Identity Theft and other threats to personal privacy
  - Equipment Theft
  - Espionage in cyberspace
  - Cyberterrorism
  - …

Kinds of Threats

Interception

- an unauthorized party (human or not) gains access to an asset

Interruption

- an asset becomes lost, unavailable, or unusable

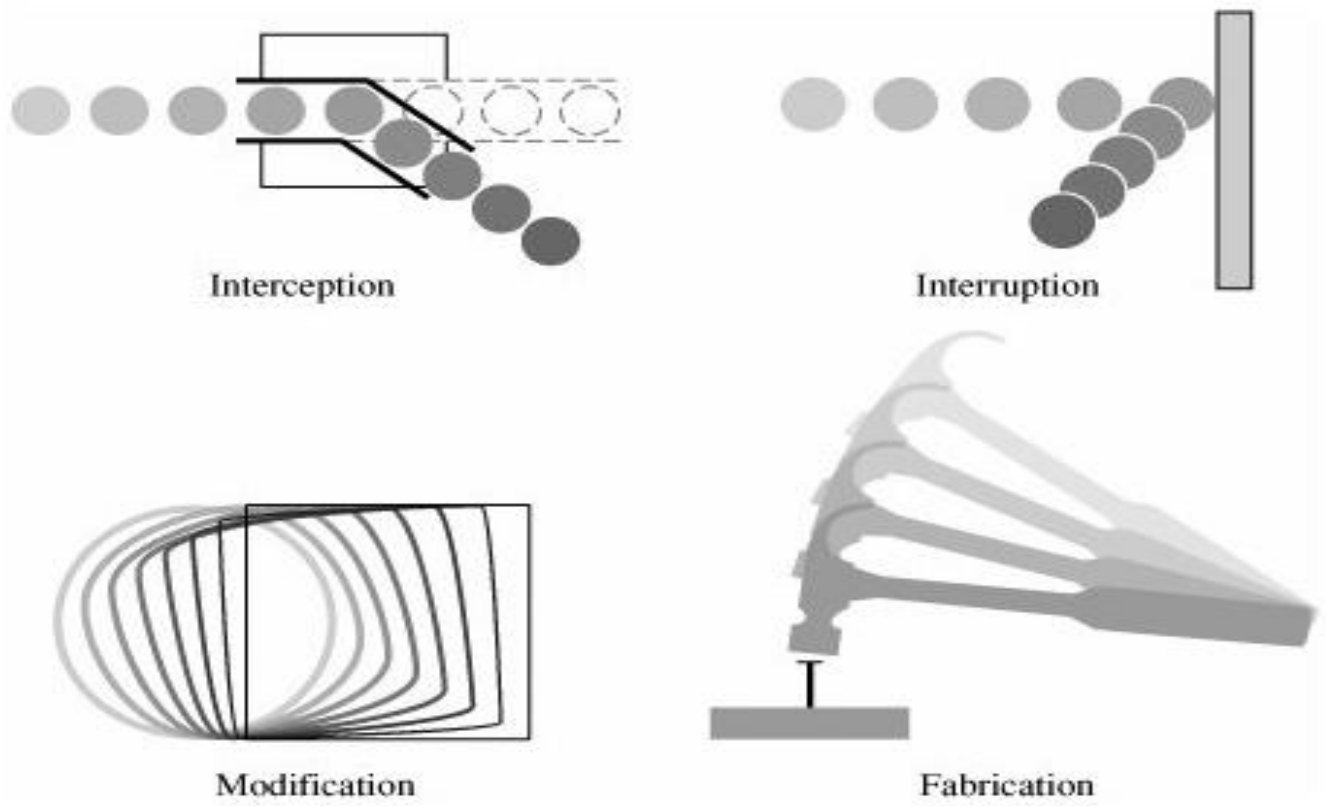
Modification

- an unauthorized party changes the state of an asset

Fabrication

- an unauthorized party counterfeits an asset

Security threats

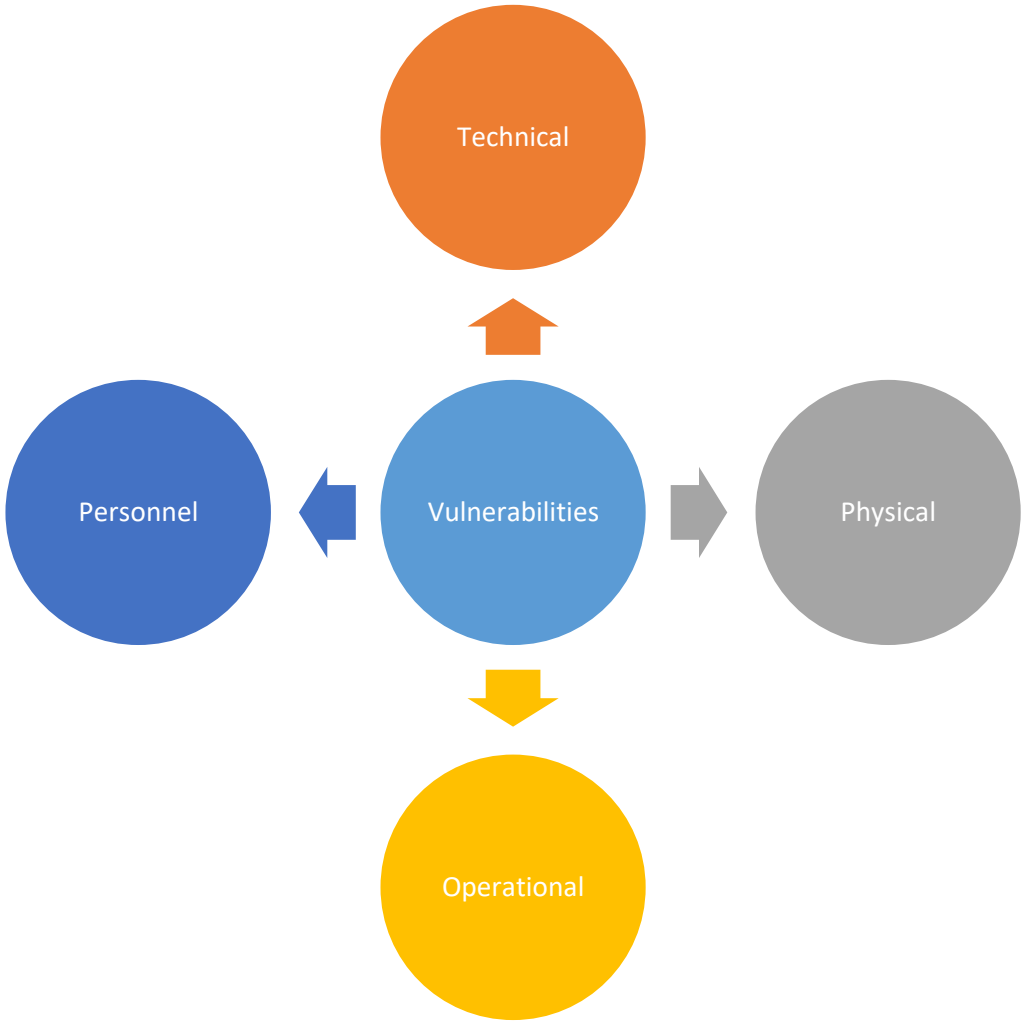


Modification

Modification

Vulnerability

- They are basically the weakness that allow the threat to exploit you.



Controls

- Controls are the means and ways to block a threat, which tries to exploit one or more vulnerabilities

Threat, vulnerability and controls

- A threat is blocked by control of vulnerability.

Example – Cyclone Biparjoy

Q: What were city vulnerabilities, threats, and controls?

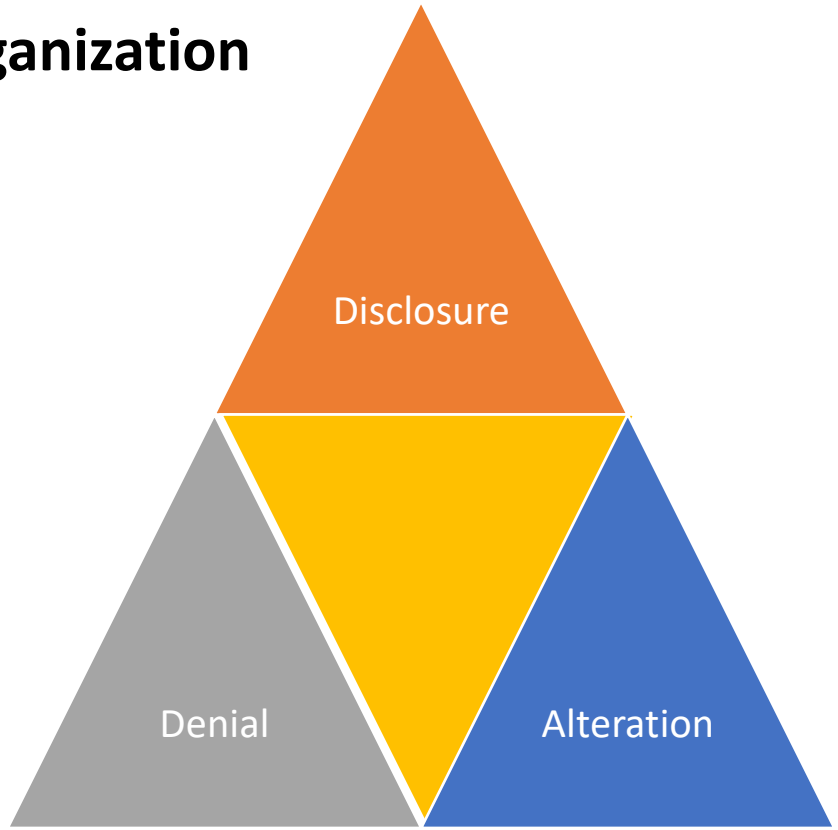
A: Vulnerabilities: Geographical location in near sea, …
Threats: hurricane, dam damage, terrorist attack, …
Controls: dams and other civil infrastructures, emergency response plan, …

- Attack (materialization of a vulnerability/threat combination)
  - = exploitation of one or more vulnerabilities by a threat; tries to defeat controls
    - Attack may be:
      - *Successful* (a.k.a. an *exploit*)
        - resulting in a breach of security, a system penetration, etc.
      - *Unsuccessful*
        - when controls block a threat trying to exploit a vulnerability

DAD Triad

Malicious individuals

- –**Goals for defeating the security of an organization**
- –**D**isclosure, **A**lteration, and **D**enial



Attacker's need MOM

Hacker Communities

- Two ways commonly used to categorize **hackers**
  - White Hat good hackers vs. Black Hat bad hackers
  - Based loosely on psychological profiling

Hat Categories

- White Hat/Black Hat model
  - White hats represent the “good guys”
  - Black hats represent the “bad guys”
- Everything the good guys do is right, legal, and justified
- “Grey Hat” hackers
  - Evidence that the dichotomy of good and evil is NOT a very good fit to the real world

HAT Classification

Black hats represent the “Bad guys”

In between white and black

White hats represent the “good guys”

New attacker categories

Red hat hackers want to save the world from evil hackers. But they choose extreme and sometimes illegal routes to achieve their goals. Red hat hackers are like the pseudo-Robin Hood of the cybersecurity field.

Blue hat hackers hack to take personal revenge for a real — or perceived — sleight from a person, employer, institution, or government.

Green hat hackers are the “newbies” in the world of hacking. Green hat hackers are not aware of the security mechanism and the inner workings of the web, but they are keen learners and determined (and even desperate) to elevate their position in the hacker community. Although their intention is not necessarily to cause harm, they may do so while “playing” with various malware and attack techniques.

Activity – Identify Hat Color

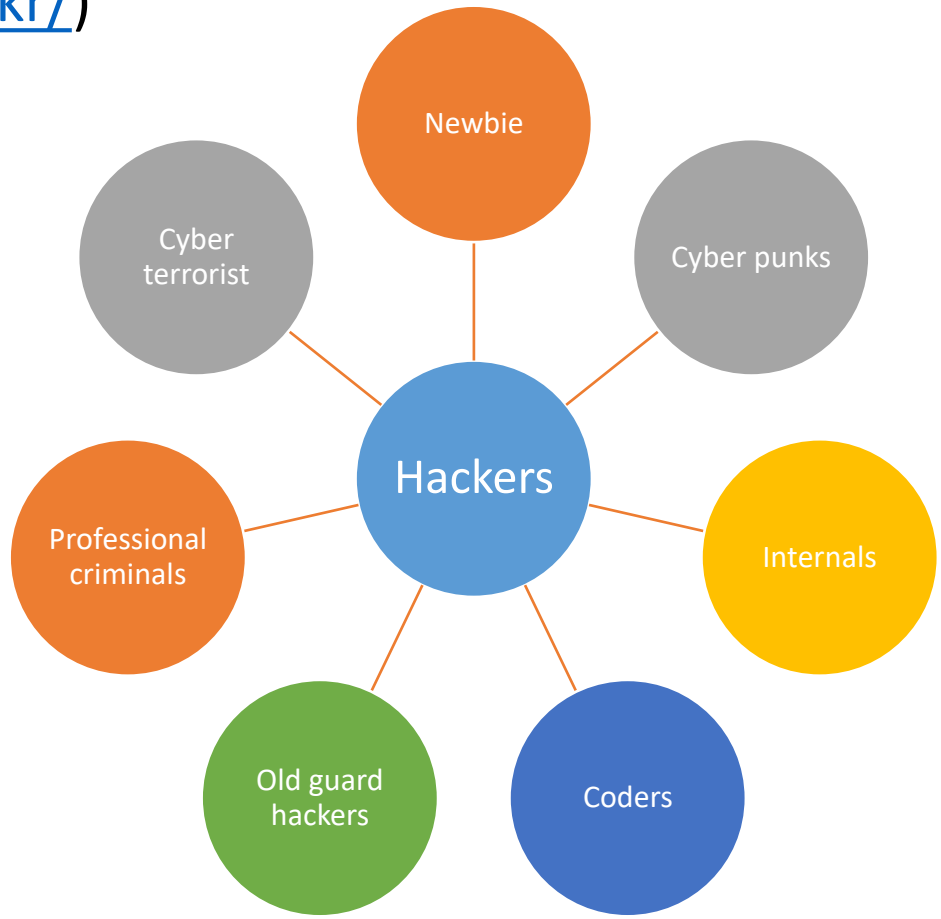
Hacker Characteristic
After hacking into ATM machines remotely using a laptop, he worked with ATM manufacturers to resolve the found security vulnerabilities.
From my laptop, I transferred $10 million to my bank account using victim account numbers and PINs after viewing recordings of victims entering the numbers.
My job is to identify weaknesses in the computer system in my company.
I used malware to compromise several corporate system to steal credit card information and sold that information to the highest bidder.
During my research for security exploits, I stumbled across a security vulnerability on a corporate network that I am authorized to access.
I am working with technology companies to fix a flaw with DNS.

Hacker Profiling

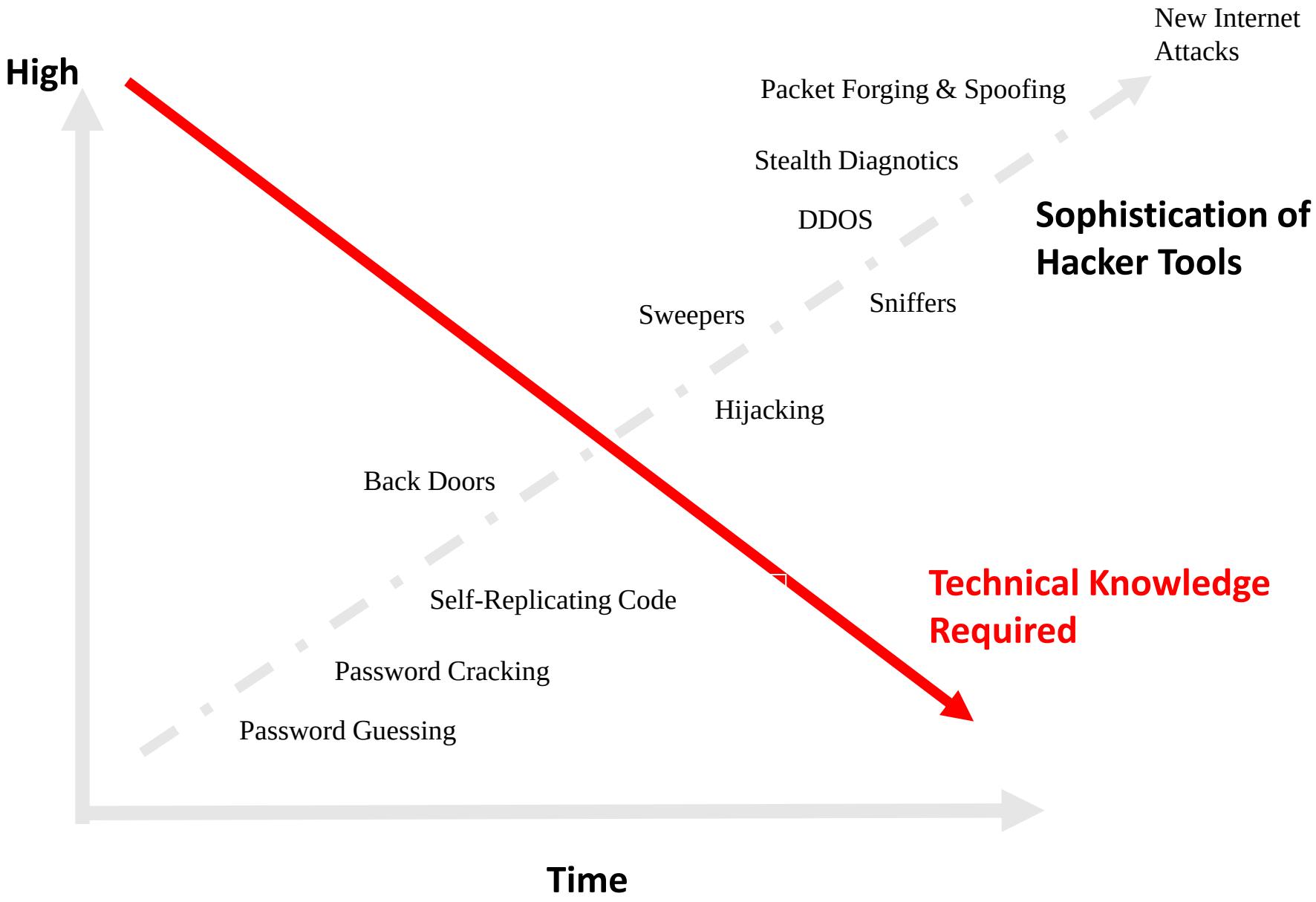
- Hacking requires that the practitioner be intimately familiar with the techniques of the perpetrator or opponent
- Reading and techniques used by both ethical and malicious hackers are identical
- Profile of a hacker is multifaceted

Hacker Profiling

- This classification is based on the work of Mark Rogers. (Source: http://homes.cerias.purdue.edu/~mkr/)



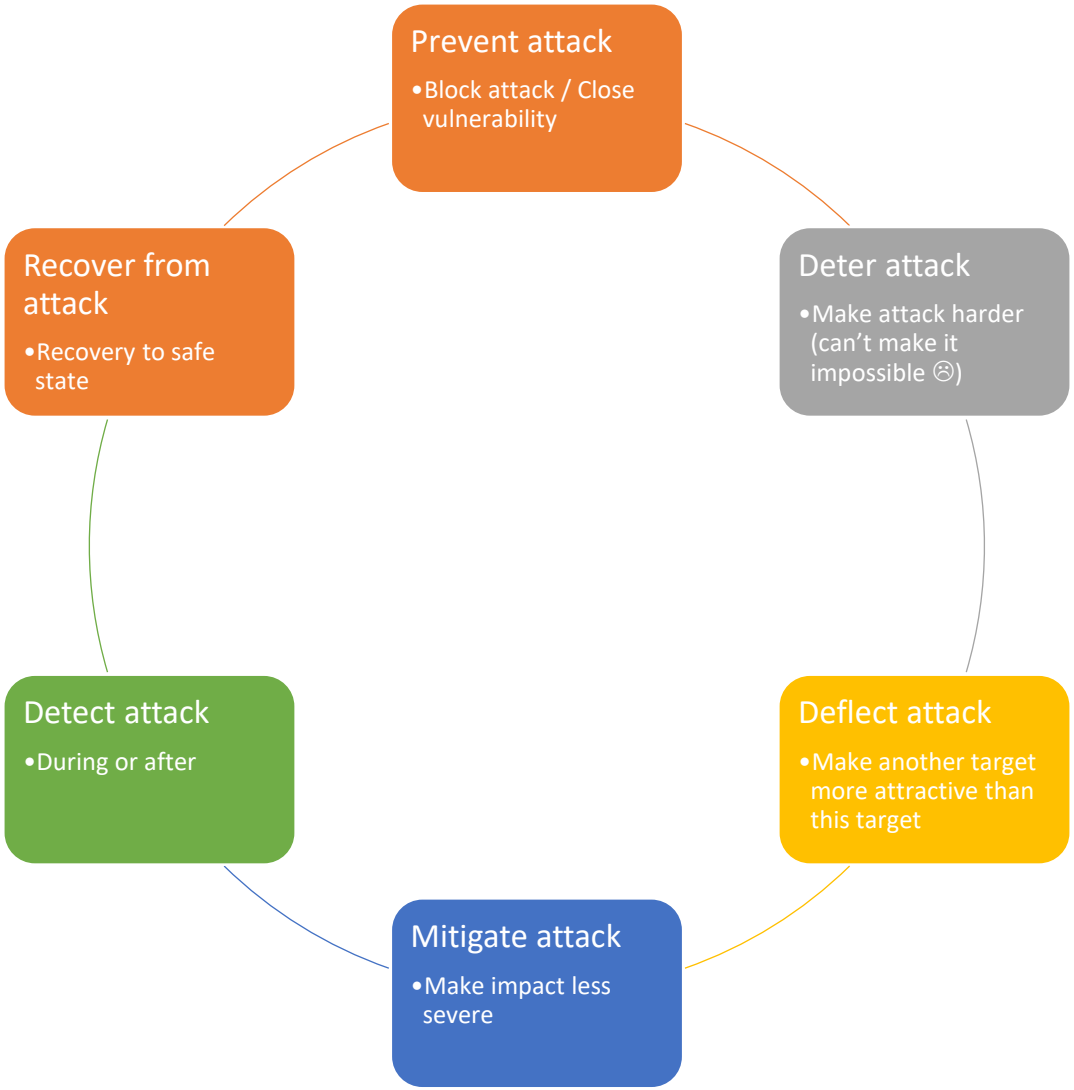
Hacker Profile	Description
Novices	Limited computer and programming skills. Rely on toolkits to conduct their attacks. Can cause extensive damage to systems because they often don't understand how attacks work. Looking for media attention.
Cyber-punks	Capable of writing their own software. Have an understanding of the systems they are attacking. Many are engaged in credit card number theft and telecommunications fraud. Have a tendency to brag about their exploits.
Internals	a) Disgruntled employees or ex-employees May be involved in technology-related jobs. Aided by privileges they have or were assigned as part of their job function. **These hackers pose the greatest security threat.** b) Petty thieves Include employees, contractors, consultants. Motivated by greed, or need to pay off habits, such as drugs or gambling. Opportunistic; take advantage of poor internal security. Computer literate.
Old guard hackers	Appear to have no criminal intent. Alarming disrespect for personal property. Appear to be interested in the intellectual endeavor.
Coders	Act as mentors to newbies. Write scripts and tools that others use. Motivated by a sense of power and prestige. Dangerous; have hidden agendas, use Trojan horses.
Professional criminals	Specialize in corporate espionage. Guns for hire. Highly motivated, highly trained, have access to state-of-the-art equipment.
Information warriors/ cyber-terrorists	Increase in activity since the fall of many Eastern Bloc intelligence agencies. Well funded. Mix political rhetoric with criminal activity. Political activists.
Hacktivists	Work to eradicate or damage entities or causes they perceive to be evil. Mix political rhetoric with criminal activity. Political activists. Engage in hacktivism.


High
New Internet Attacks
Packet Forging & Spoofing
Stealth Diagnotics
DDOS
Sophistication of Hacker Tools
Sniffers
Sweepers
Hijacking
Back Doors
Technical Knowledge Required
Self-Replicating Code
Password Cracking
Password Guessing
Time

Identify Hacker Type

Description	Hacker type
Google's for a DoS tools and runs the tool without understanding	
Hacks the website to promote political agenda	
Develops hacking tools and are motivated by power and prestige	
Sells hacking service for monetary gains	
Destroys electric power grid to create disruption	
Employees steals IP of the company and sells it to its competitors	
Installs a logic bomb before leaving the office	

Methods of Defense



Controls

- Castle in Middle Ages
  - Location with natural obstacles
  - Heavy walls
    - Arrow slits
    - Crenellations
  - Strong gate
    - Tower
  - Guards / passwords

- Computers Today
  - Encryption
  - Software controls
  - Hardware controls
  - Policies and procedures
  - Physical controls

- Medieval castles
  - location (steep hill, island, etc.)
  - moat / drawbridge / walls / gate / guards /passwords
  - another wall / gate / guards /passwords
  - yet another wall / gate / guards /passwords
  - tower / ladders up

- Multiple controls in computing systems can include:
  - system perimeter – defines „inside/outside”
  - preemption – attacker scared away
  - deterrence – attacker could not overcome defenses
  - faux environment (e.g. honeypot, sandbox) – attack deflected towards a worthless target (but the attacker doesn't know about it!)

→Note layered defense / multilevel defense / defense in depth (ideal!)

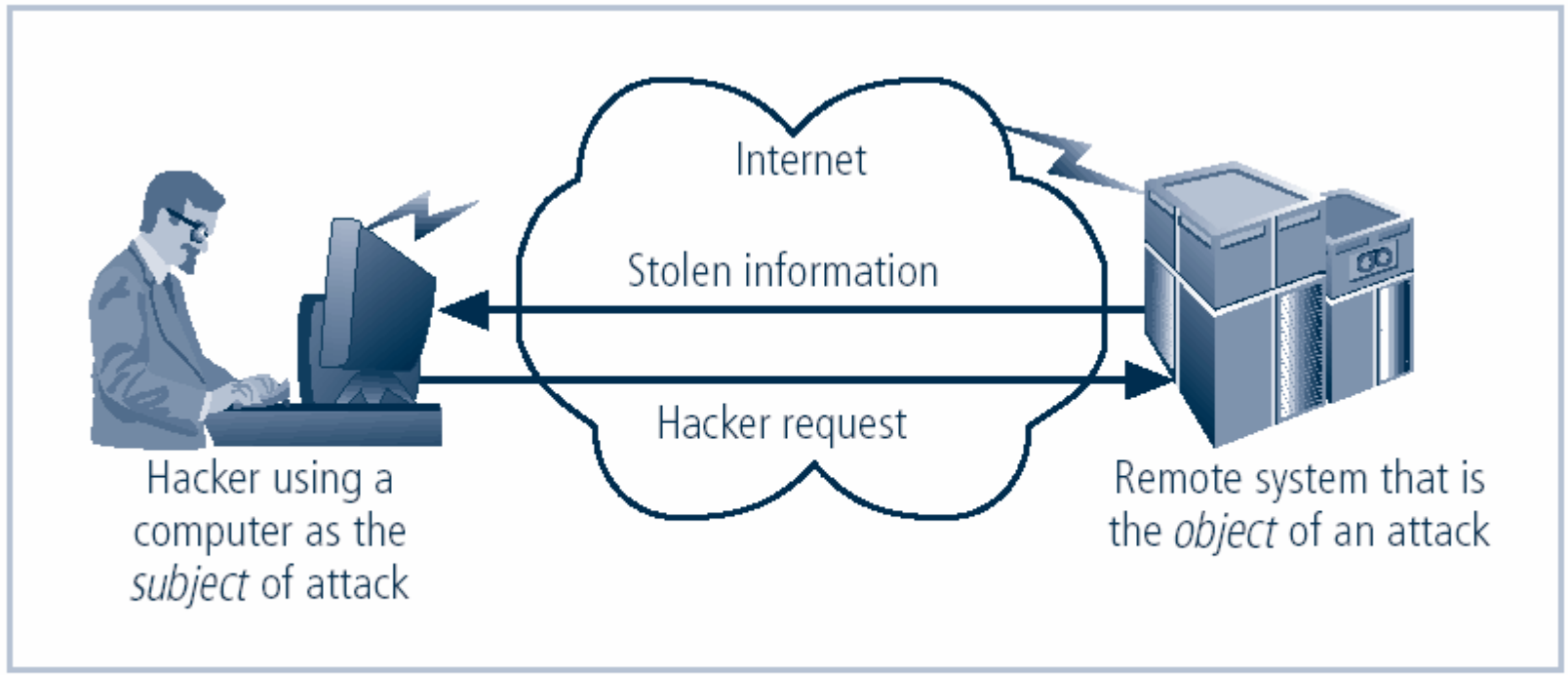
Components of an Information System

- Information system (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization

Securing Components

- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked

Subject and Object of Attack

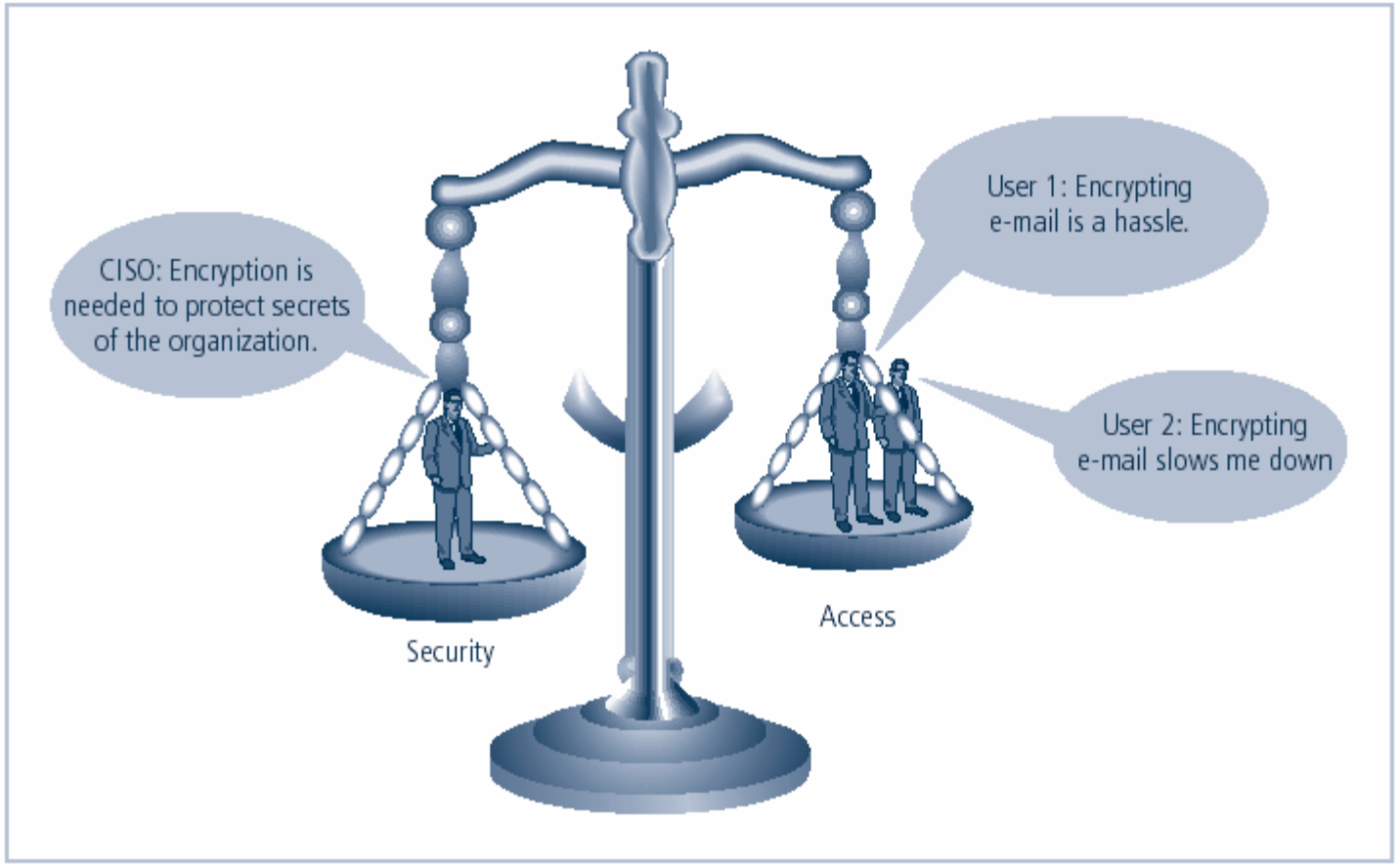


Computer as the Subject and Object of an Attack

Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats

Balancing Security and Access



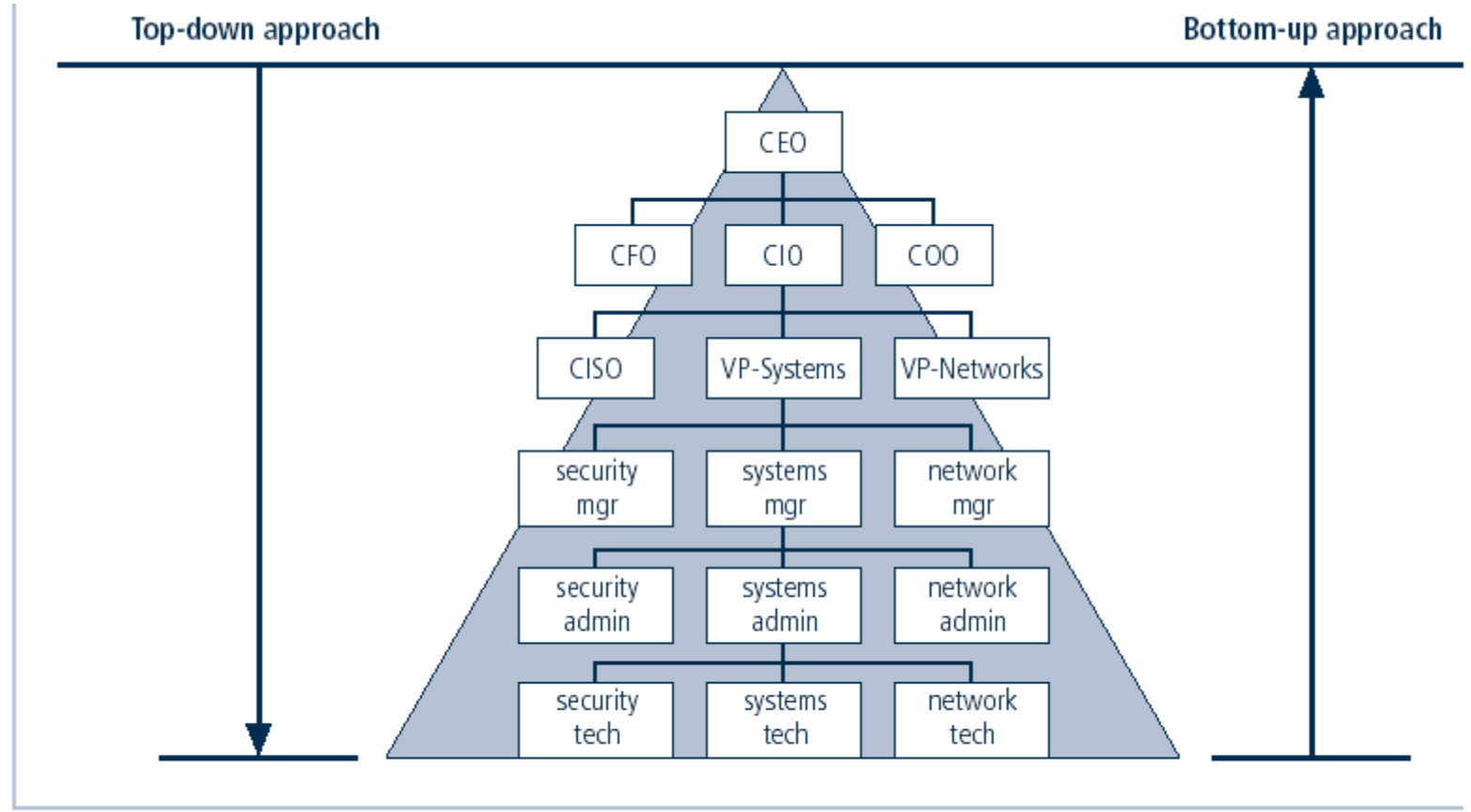
Balancing Information Security and Access

Approaches to Information Security Implementation: Bottom-Up Approach

- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power

Approaches to Information Security Implementation: Top-Down Approach

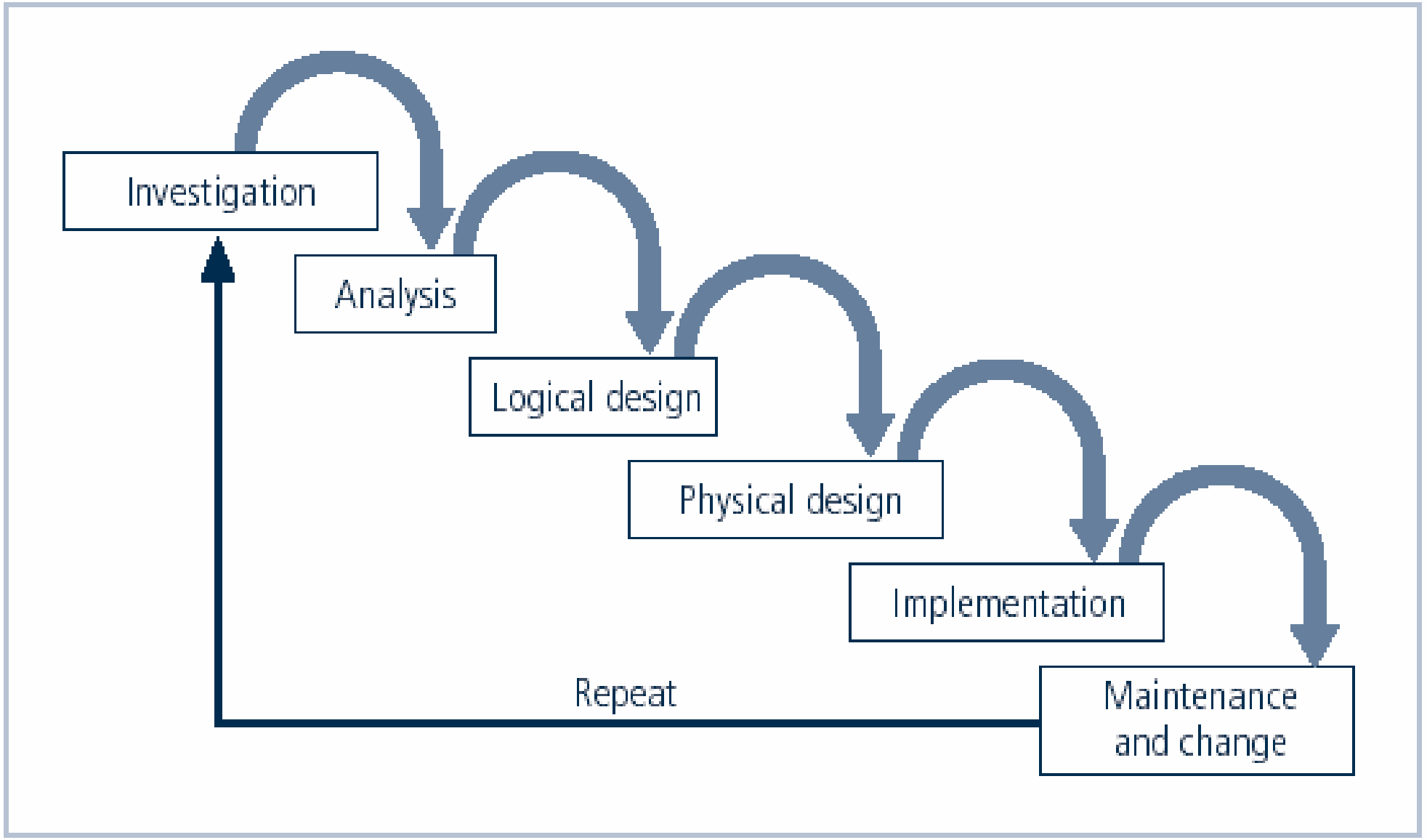
- Initiated by upper management
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful top-down approach also involve formal development strategy referred to as systems development life cycle



Approaches to Information Security Implementation

The Systems Development Life Cycle

- Systems Development Life Cycle (SDLC) is methodology for design and implementation of information system within an organization
- Methodology is formal approach to problem solving based on structured sequence of procedures
- Using a methodology:
  - Ensures a rigorous process
  - Avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases



SDLC Waterfall Methodology

Investigation

- What problem is the system being developed to solve?
- Objectives, constraints, and scope of project are specified
- Preliminary cost-benefit analysis is developed
- At the end, feasibility analysis is performed to assess economic, technical, and behavioral feasibilities of the process

Analysis

- Consists of assessments of the organization, status of current systems, and capability to support proposed systems
- Analysts determine what new system is expected to do and how it will interact with existing systems
- Ends with documentation of findings and update of feasibility analysis

Logical Design

- Main factor is business need; applications capable of providing needed services are selected
- Data support and structures capable of providing the needed inputs are identified
- Technologies to implement physical solution are determined
- Feasibility analysis performed at the end

Physical Design

- Technologies to support the alternatives identified and evaluated in the logical design are selected
- Components evaluated on make-or-buy decision
- Feasibility analysis performed; entire solution presented to end-user representatives for approval

Implementation

- Needed software created; components ordered, received, assembled, and tested
- Users trained and documentation created
- Feasibility analysis prepared; users presented with system for performance review and acceptance test

Maintenance and Change

- Consists of tasks necessary to support and modify system for remainder of its useful life
- Life cycle continues until the process begins again from the investigation phase
- When current system can no longer support the organization’s mission, a new project is implemented

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Investigation

- Identifies process, outcomes, goals, and constraints of the project
- Begins with Enterprise Information Security Policy (EISP)
- Organizational feasibility analysis is performed

Analysis

- Documents from investigation phase are studied
- Analysis of existing security policies or programs, along with documented current threats and associated controls
- Includes analysis of relevant legal issues that could impact design of the security solution
- Risk management task begins

Logical Design

- Creates and develops blueprints for information security
- Incident response actions planned:
  - Continuity planning
  - Incident response
  - Disaster recovery
- Feasibility analysis to determine whether project should be continued or outsourced

Physical Design

- Needed security technology is evaluated, alternatives are generated, and final design is selected
- At end of phase, feasibility study determines readiness of organization for project

Implementation

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues evaluated; specific training and education programs conducted
- Entire tested package is presented to management for final approval

Maintenance and Change

- Perhaps the most important phase, given the ever-changing threat environment
- Often, reparation and restoration of information is a constant duel with an unseen adversary
- Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve

NIST CSF 2.0

Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CSF components

CSF Core

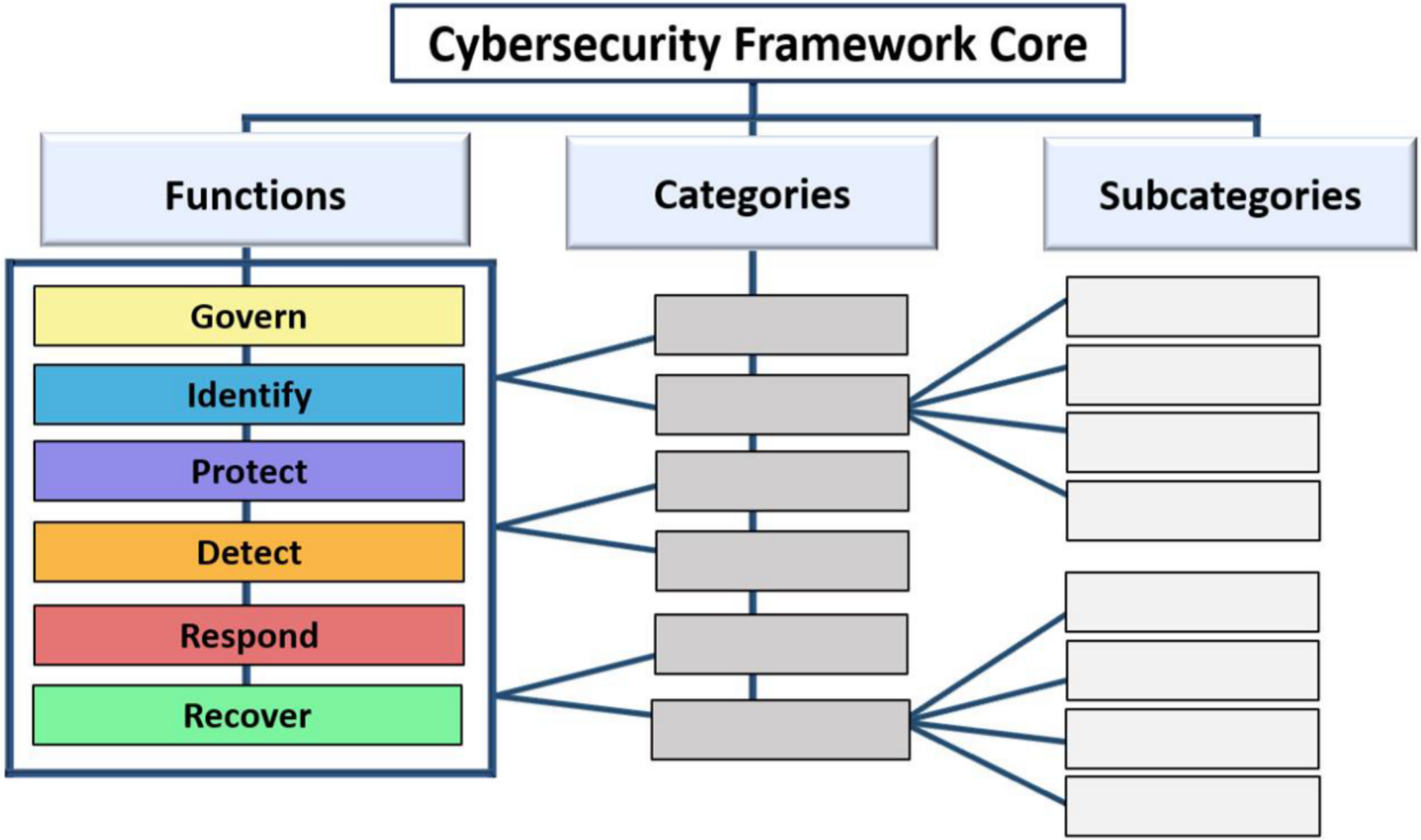
- Taxonomy of high-level cybersecurity outcomes
- Hierarchy: Functions, Categories, Subcategories

CSF Organizational Profiles

- Describe current/target cybersecurity posture
- Based on CSF Core outcomes

CSF Tiers

- Classify cybersecurity risk management rigor
- Provide context for risk views and processes

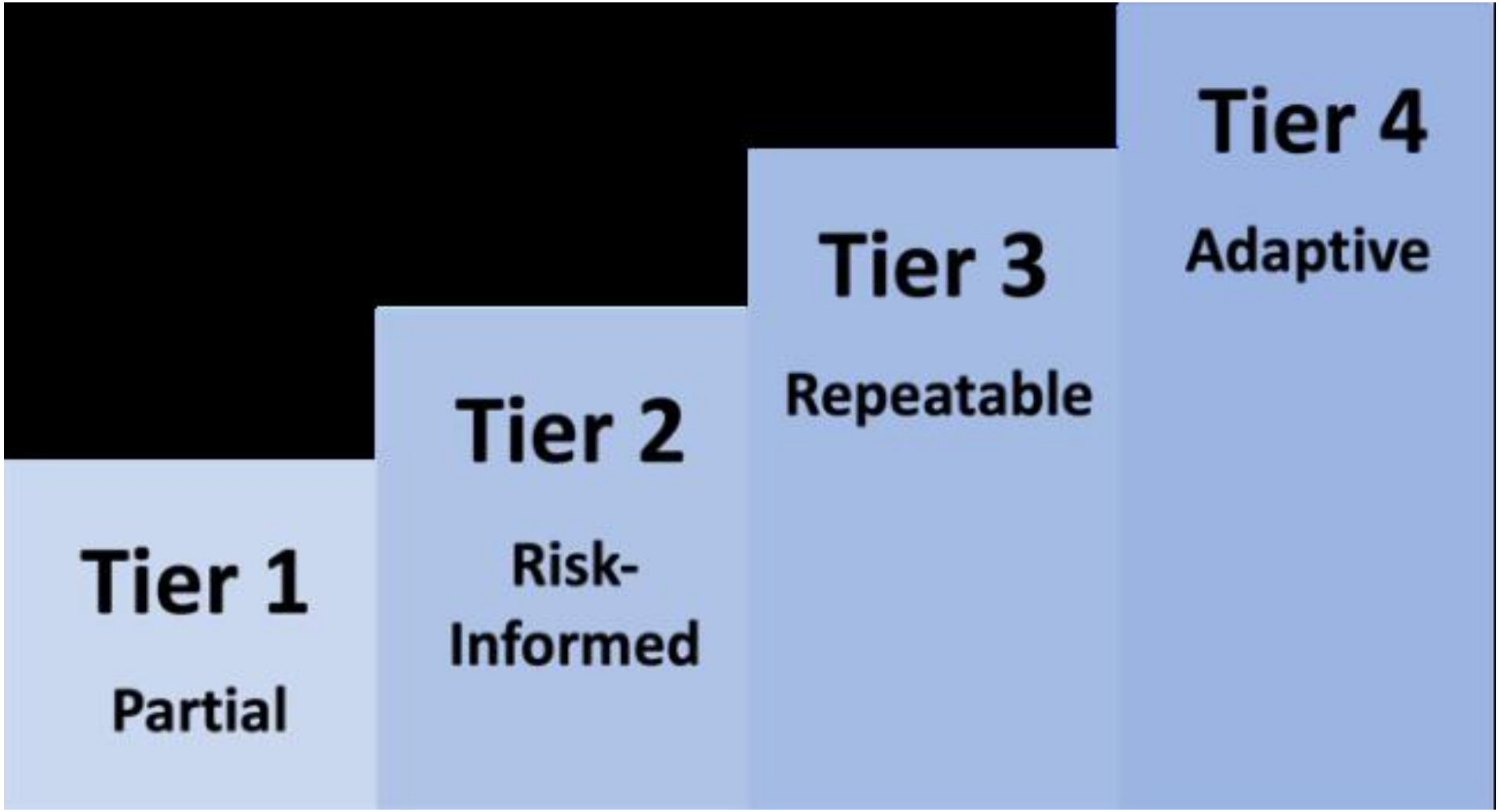

Cybersecurity Framework Core
Functions
Categories
Subcategories
Govern
Identify
Protect
Detect
Respond
Recover

CSF Core

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Steps for creating and using a CSF Organizational Profile

CSF Tiers for cybersecurity risk governance and management



ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance
10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (7)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Internal Image
- Modify Authentication Process (4)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (7)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (7)
- Valid Accounts (4)

Defense Evasion
39 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (7)
- Hijack Execution Flow (11)
- Impair Defenses (7)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (5)
- Pre-OS Boot (5)
- Process Injection (11)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (6)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities

Credential Access
15 techniques

- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (7)

Discovery
27 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account