Chapter 1: Intro to Network Security Management

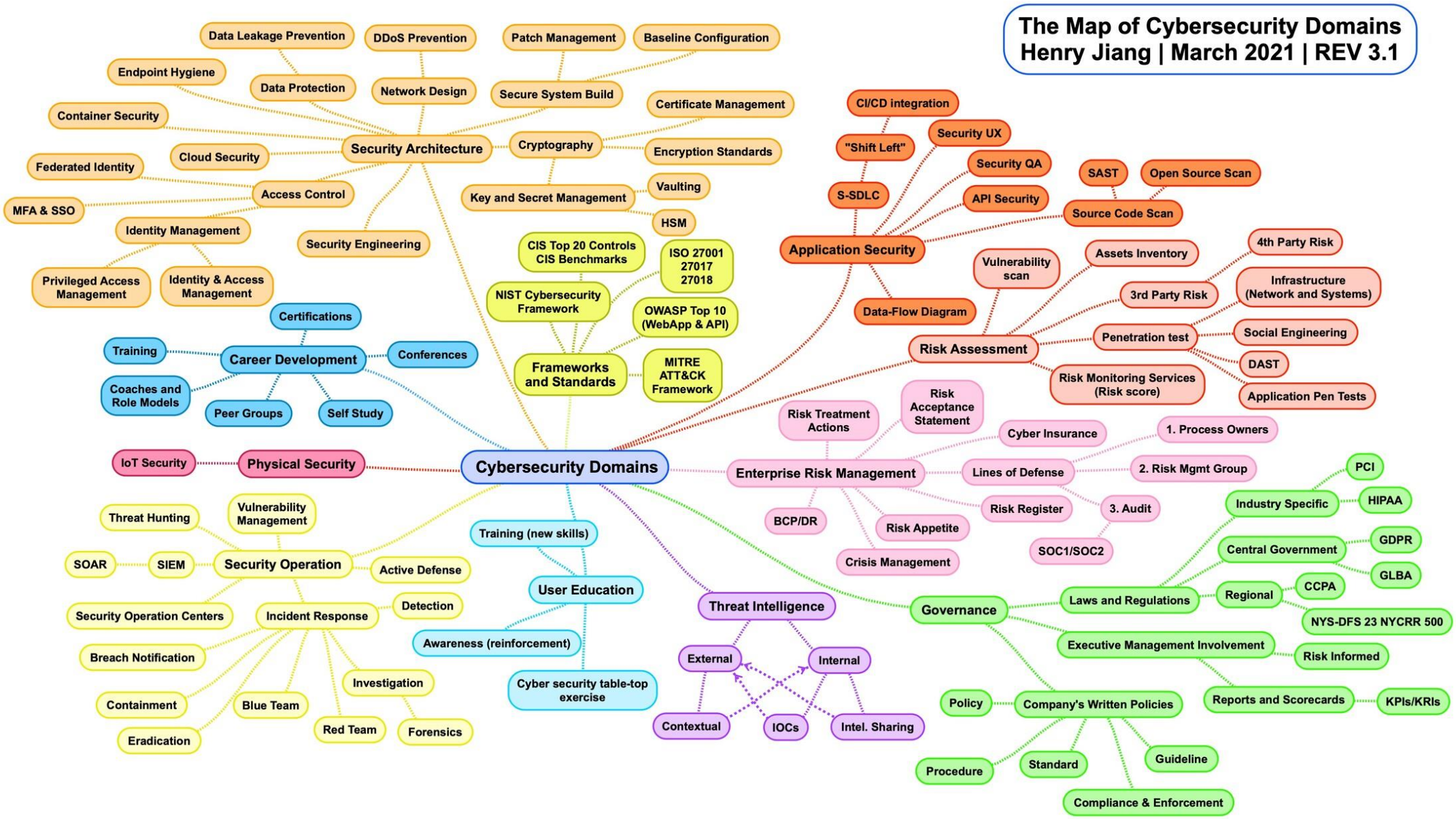
Gonzalo De La Torre Parra, Ph.D.

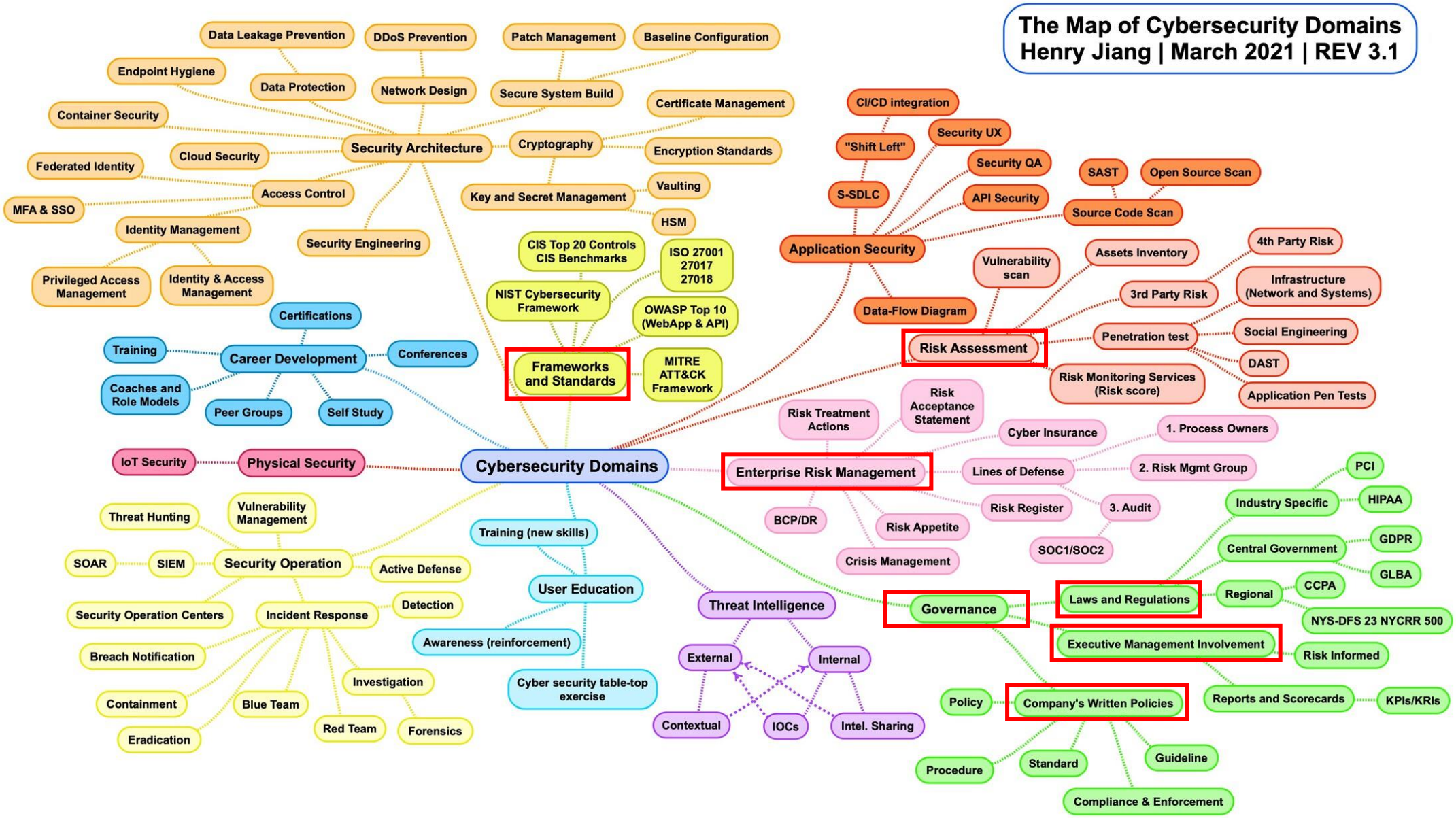
Fall 2021

Overview

Security management is one of the most overlooked domains, yet almost nothing we do in the other domains means anything without it. Security management is made up of several tasks:

- Risk assessments, which is the process we use to identify risks to the organization and systemically identify methods to combat those risks, usually relying on input from experts in the below domains
- Overseeing the processes for other security functions to ensure those align with business/operations processes
- Change management processes and procedures in place
- User security awareness training


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Endpoint Hygiene
Data Protection
Network Design
Container Security
Cloud Security
Federated Identity
Access Control
MFA & SSO
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Physical Security
IoT Security
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Security Operation Centers
Incident Response
Detection
Breach Notification
Containment
Eradication
Blue Team
Red Team
Investigation
Forensics
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
Secure System Build
Patch Management
Baseline Configuration
Cryptography
Certificate Management
Encryption Standards
Key and Secret Management
Vaulting
HSM
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
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engineering
DAST
Application Pen Tests
Risk Monitoring Services (Risk score)
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
3. Audit
Risk Register
BCP/DR
Risk Appetite
Crisis Management
SOC1/SOC2
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
Regional
CCPA
GLBA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Reports and Scorecards
KPIs/KRIs
Company's Written Policies
Policy
Procedure
Standard
Guideline
Compliance & Enforcement
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Cyber security table-top exercise


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Container Security
Certificate Management
Cloud Security
Cryptography
Encryption Standards
Federated Identity
Access Control
Key and Secret Management
Vaulting
MFA & SSO
HSM
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Application Security
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Data-Flow Diagram
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engineering
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
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
3. Audit
Risk Register
BCP/DR
Risk Appetite
Crisis Management
SOC1/SOC2
Physical Security
IoT Security
Security Operation
Vulnerability Management
Threat Hunting
SOAR
SIEM
Active Defense
Incident Response
Detection
Security Operation Centers
Breach Notification
Containment
Eradication
Blue Team
Red Team
Investigation
Forensics
Training (new skills)
User Education
Awareness (reinforcement)
Cyber security table-top exercise
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
Reports and Scorecards
KPIs/KRIs
Policy
Company's Written Policies
Procedure
Standard
Guideline
Compliance & Enforcement

Motivation – Network Security Management

- Digitalization of resources
- Decentralization of information processing (Federated, Decentralized)
- Global business environment (More users, networks, protocols, and technologies)
- Dynamic business place
  - Work while traveling
  - Work from home
- Novel technologies with weak computational resources and security systems (E.g. IoT)

Acknowledging the problem

- Information security is recognized as an imperative vehicle by which the organization's information assets are secured.
- Security is not only responsibility of a dedicated group. All employees are responsible.
- New units and positions are created to focus on this task (E.g. Information Security Managers and Teams)

Key terms: Speaking the same language

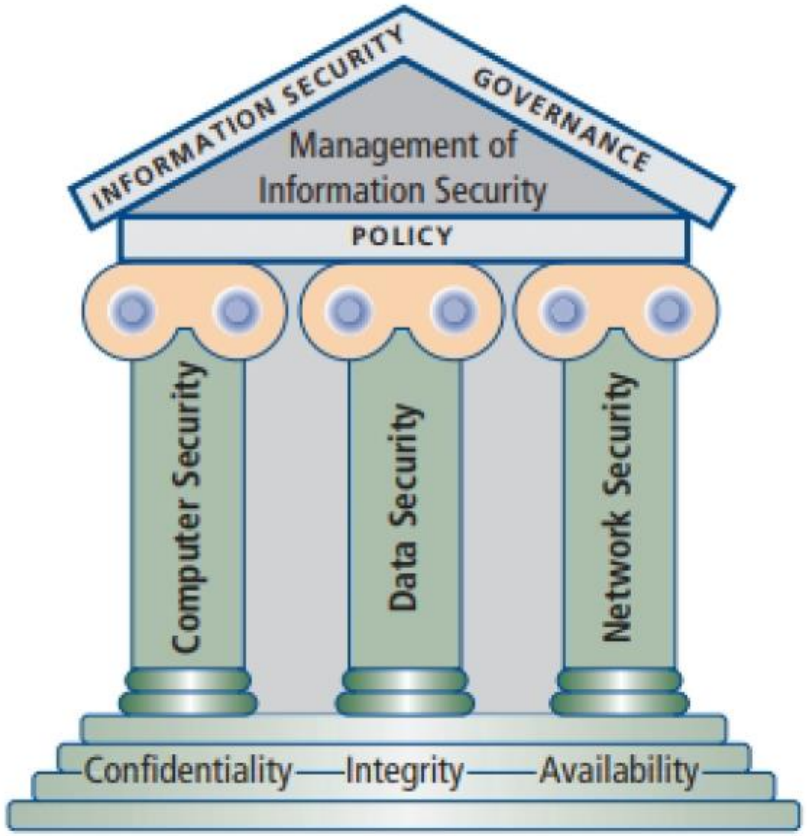
- **Asset:** An organizational resource that is being protected. E.g., Web site, software information, data, a person, computer system, hardware, etc. Assets, particularly information assets, are the focus of what security efforts are attempting to protect.
- **Information asset**: The focus of information security; information that has value to the organization, and the systems that store, process, and transmit the information.
- **Information security (InfoSec):** Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.
- Security: A state of being secure and free from danger

Specialized Security Areas

- Physical Security
- Operation Security
- Communications Security
- Cyber Security: The protection of computerized information processing systems and the data they contain and process.
- Network Security: A subset of communications security and cybersecurity; the protection of voice and data networking components, connections, and content.

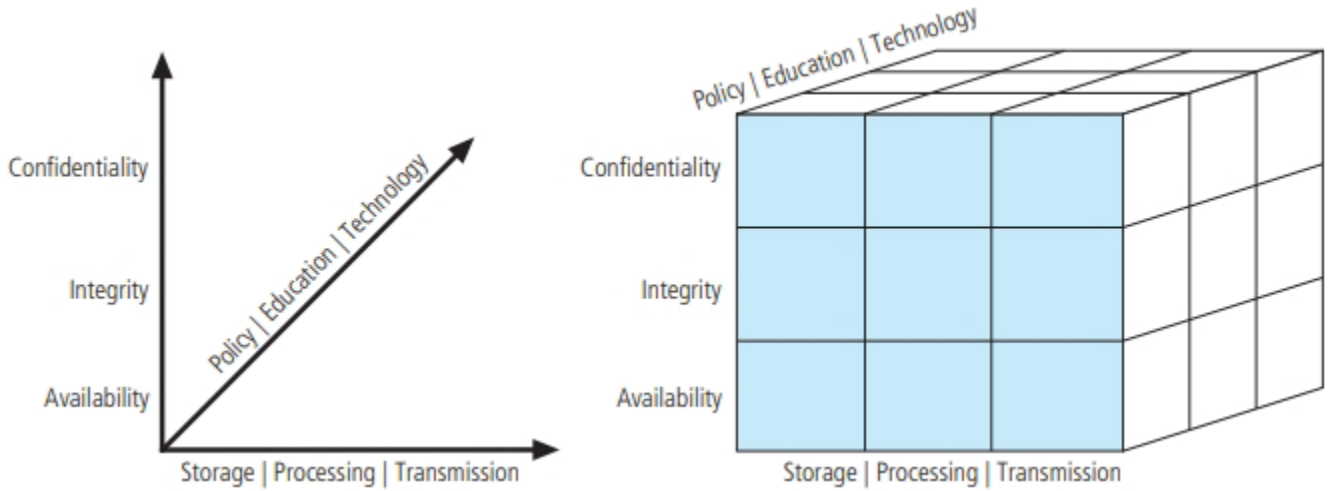
Information Security as defined by the Committee on National Security Systems {CNSS)

- Information security (InfoSec) focuses on the protection of information and the characteristics that give it value, such as confidentiality, integrity, and availability, and includes the technology that houses and transfers that information through a variety of protection mechanisms such as policy, training and awareness programs, and technology.



CNSS Security Model - McCumber Cube

- Comprehensive Model of InfoSec that serves as the standard for understanding many aspects of InfoSec, and shows the three dimensions that are central to the discussion of InfoSec: information characteristics, information location, and security control categories.



- You must make sure that each of the 27 cells is properly addressed by each of the three communities of interest.
- E.g. Technology, integrity, and storage
  - Controls to protect information such as host intrusion detection and prevention systems.

CIA Triad

- Information security revolves around the three key principles: confidentiality, integrity and availability (CIA).
- Key characteristics of information that make it valuable to an organization

What is Confidentiality?

- Confidentiality measures are designed to protect against unauthorized disclosure of information. The objective of the confidentiality principle is to ensure that private information remains private and that it can only be viewed or accessed by individuals who need that information in order to complete their job duties.

What is Confidentiality?

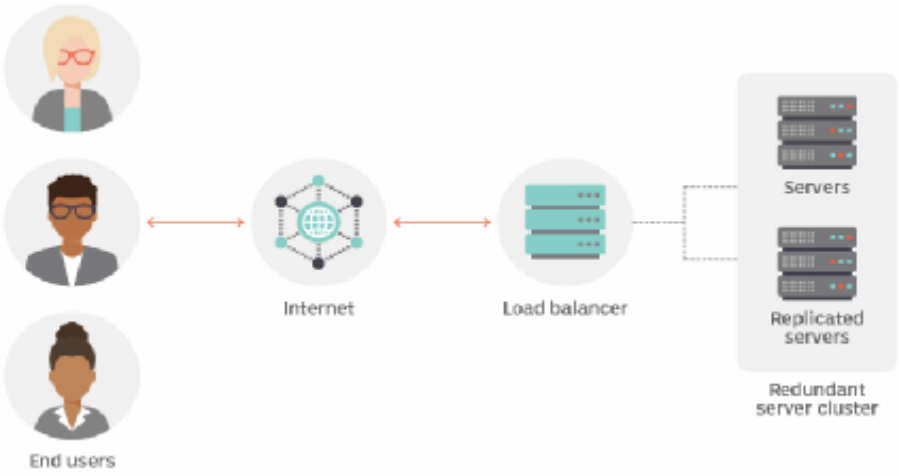
- While U.S. federal agencies have had lapses that resulted in unwanted data disclosures, an event in July 2015 eclipsed all previous similar lapses.
- The loss of 21.5 million federal background-check files rocked the Office of Personnel Management (OPM)
- Revealing names, addresses, financial records, health data, and other sensitive private information
- Chinese hackers (Believed to be responsible)

What is Integrity?

- Integrity involves protection from unauthorized modifications (e.g., add, delete, or change) of data. The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified.

What is availability?

- Availability is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users. The objective of availability is to ensure that data is available to be used when it is needed to make decisions.



Additional Characteristics

- Privacy: Information that is collected, used, and stored by an organization should be used only for the purposes stated by the data owner at the time it was collected.
- Identification: An information system possesses the characteristic of identification when it is able to recognize individual users.
- Authentication: Authentication is the process by which a control establishes whether a user (or system) is the entity it claims to be.
- Authorization: After the identity of a user is authenticated, a process called authorization defines what the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to do, such as access, modify, or delete the contents of an information asset.
- Accountability of information: occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.

Key Terms

accountability The access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability.

authentication The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

authorization The access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels.

availability An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

C.I.A. triad The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

confidentiality An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

disclosure In information security, the intentional or unintentional exposure of an information asset to unauthorized parties.

identification The access control mechanism whereby unverified entities who seek access to a resource provide a label by which they are known to the system.

information aggregation The collection and combination of pieces of nonprivate data, which could result in information that violates privacy. Not to be confused with aggregate information.

integrity An attribute of information that describes how data is whole, complete, and uncorrupted.

privacy In the context of information security, the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality.

The 12 Categories of Threats

Table 1-1 The 12 Categories of Threats to Information Security[5]

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Threats and Attacks

Key Terms

attack An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.

exploit A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain.

loss A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use.

threat Any event or circumstance that has the potential to adversely affect operations and assets. The term *threat source* is commonly used interchangeably with the more generic term *threat*. While the two terms are technically distinct, in order to simplify discussion the text will continue to use the term *threat* to describe threat sources.

threat agent The specific instance or a component of a threat.

threat event See *attack*.

vulnerability A potential weakness in an asset or its defensive control system(s).

Compromises to Intellectual Property

- Software piracy
- Copyright protection and user registration

Deviations in Quality of Service

- Internet service issues
- Communications and other service provider issues
- Power irregularities

Espionage or Trespass

- Novice Hackers: have little or no real expertise of their own, but rely upon the expertise of expert hackers, who often become dissatisfied with attacking systems directly and turn their attention to writing software. These programs are automated exploits that allow novice hackers to act as script kiddies or packet monkeys.

- Professional Hackers: usually a master of several programming languages, networking protocols, and operating systems, and exhibits a mastery of the technical environment of the chosen targeted system. Once an expert hacker chooses a target system, the likelihood is high that he or she will successfully enter the system.

- Password Attacks
  - Brute Force
  - Dictionary Attacks
  - Social Engineering

Forces of Nature

- Forces of nature, sometimes called acts of God, can present some of the most dangerous threats because they usually occur with little warning and are beyond the control of people.
- These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only people's lives but also the storage, transmission, and use of information.

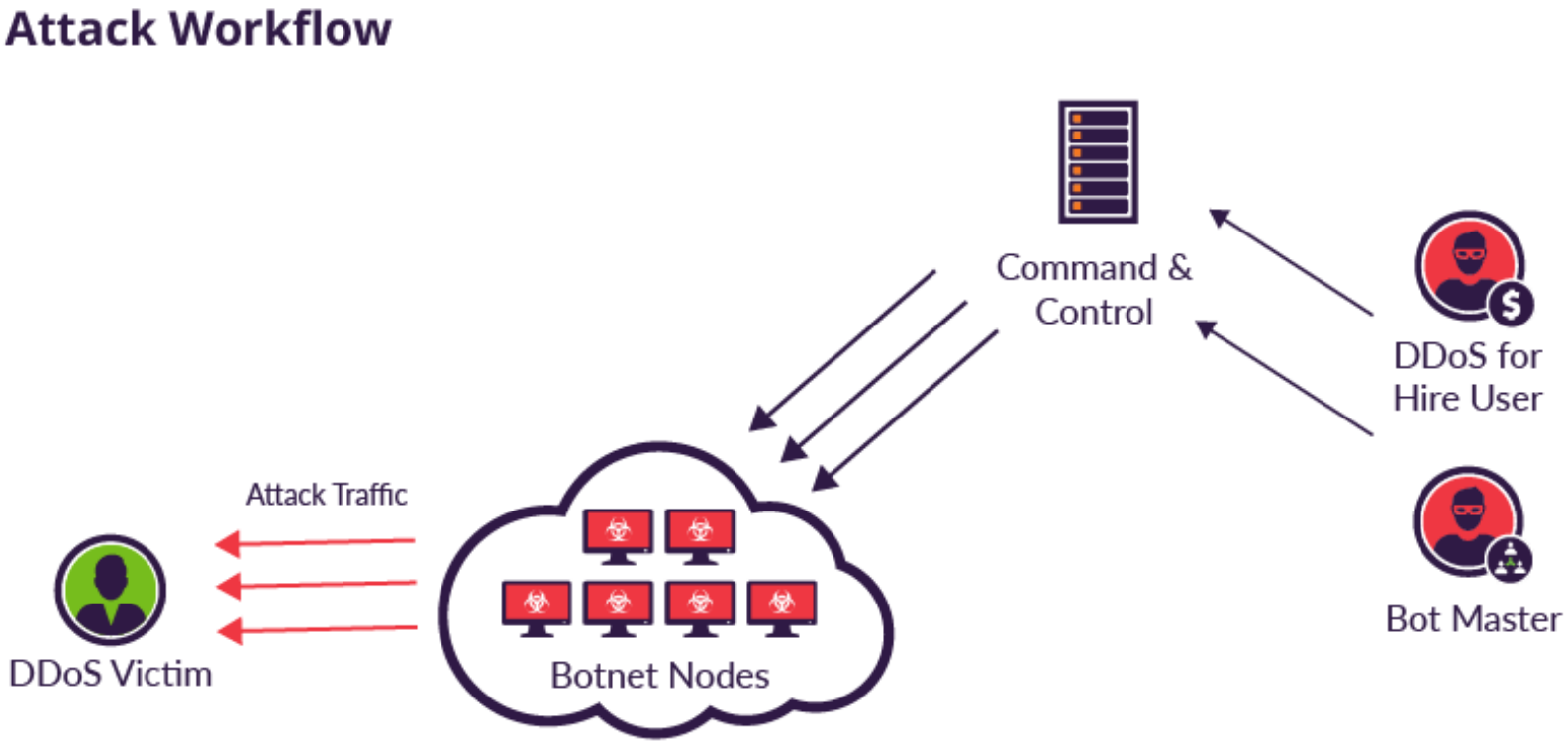
Software Attacks

- Malware – Referred to as malicious code or malicious software. Malicious code attacks include the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- Polymorphic Malware - A polymorphic threat that evolves, changing its size and other external file characteristics to elude detection by antivirus software programs.

Software Attacks

- Back doors - A malware payload that provides access to a system by bypassing normal access controls.
- Bot - Automated software program that executes certain commands when it receives a specific input.
- DoS - An attack that attempts to overwhelm a computer ta rget's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.
- Man-in-the-Middle - Group of attacks whereby a person intercepts a communications stream and inserts himself in the conversation to convince each of the legitimate parties that the attacker is the other communications partner

E.g. Botnet



https://github.com/epsylon/ufonet
https://github.com/malwaredllc/byob

Human Error or Failure

- Advance-fee fraud (AFF) – the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer
- Phishing - Contains hidden or embedded code that redirects the reply to a third-party site to extract personal or confidential information
- Social Engineering: Convince people to reveal credentials
- Spear phishing: Targeted phishing attacks

Information Extortion and Ransomware

- Information extortion – Threat to reveal stolen information

- Ransomware – Software that encrypts valuable information. This approach is used to extort a victim and ask for a payment in exchange of the decryption key.
  - Colonial pipeline: 4.4 Billion
  - CWT: 4.5 million

Ransomware Example

Sabotage and Vandalism

- Cyber activist and hacktivist - A hacker who seeks to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.
- Cyber terrorism - The conduct of terrorist activities by online attackers.
- Cyber warfare - Formally sanctioned offensive operations conducted by a government or state against information or systems of another government or state. Sometimes called information warfare.

Technological Obsolescence

- Windows 7
- Windows Vista
- Windows XP
- Signature-based Intrusion Detection Systems (Stand Alone)

Management and Leadership

Management Definition

- Management - The art of using the resources to get the job done
- Manager - A member of the organization assigned to marshal and administer resources, coordinate the completion of tasks, and handle the many roles necessary to complete the desired objectives.