WEEK 2

ADVANCED INFORMATION ASSURANCE AND SECURITY

THREAT ENVIRONMENT

- The threat environment consists of the type of attackers and attacks that companies face.

THE SECURITY GOALS

- **CONFIDENTIALITY**- Security goal refers to people who are authorized to use information, and are not prevented from doing so.
- **INTEGRITY-** attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network.
- **AVAILABILITY**- People who are authorized to use information are not prevented from doing so.

COMPROMISES - It refers to when a threat succeeds in causing harm to a business.

COUNTERMEASURES- tools used to thwart attacks. It is also called safeguards and controls.

TYPE OF COUNTERMEASURES

1. **PREVENTIVE-** Preventive countermeasures keep attacks from succeeding.
2. **DETECTIVE-** identify when a threat is attacking and especially when it is succeeding. Fast detection can minimize damage.
3. **CORRECTIVE-** A countermeasure which gets the business process back on track after a compromise.

EMPLOYEES AND EX-EMPLOYEES THREAT

EMPLOYEES AND EX-EMPLOYEES ARE VERY DANGEROUS FOR FOUR REASONS:

- They have extensive knowledge of systems.
- They often have the credentials needed to access sensitive data.
- They know corporate control mechanisms and how to avoid detention.
- Companies tend to trust their employees.

EMPLOYEES SABOTAGE

- Destruction of hardware, software, or data.
- Plant time bomb or logic bomb on computer
- Sabotage can also have financial motives.

EMPLOYEE HACKING

- Hacking is intentionally accessing a computer resource without authorization or in excess of authorization.

EMPLOYEE FINANCIAL THEFT

- Misappropriation of assets
- Theft of money

THEFT OF INTELLECTUAL PROPERTY (IP)

- Copyright and patents (formally protected)
- Trade secrets: plans, product formulations, business processes, and other info that a company wishes to keep secret from competitors.

EMPLOYEE EXTORTION

- The perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest.

SEXUAL OR RACIAL HARASSMENT OF OTHER EMPLOYEES

- Via e-mail
- Displaying pornographic material

MALWARE

Malware is the generic name for any “evil software.”

- **VIRUSES-** A type of malicious software that attaches itself to a legitimate program or file and spreads when the infected program is executed.
- **WORMS**- A type of malicious software that replicates itself and spreads independently across networks without needing to attach to a host program or file. Worms typically exploit vulnerabilities in software or operating systems to propagate and can cause widespread damage by consuming network bandwidth and resources.
- **BLENDED THREATS**- A type of cyberattack that combines multiple methods, such as viruses, worms, Trojans, and other malicious techniques, to exploit vulnerabilities in a system. These threats often use a combination of different attack vectors to maximize their impact and evade detection, making them more complex and harder to defend against.
- **PAYLOADS**- Refers to the part of malware attacks that performs the malicious action once the malware has successfully infiltrated a target system.
- **TROJAN HORSES-** Malicious software disguised as a legitimate program, tricking users into executing it. Once activated, it can steal data, install malware, or open backdoors for attackers.
- **DOWNLOADERS-** A type of malware designed to download and install additional malicious software onto a system. Once executed, downloaders fetch other malware from a remote server to further infect the system.
- **SPYWARE-** A type of malware that secretly monitors and collects information about a user's activities, such as browsing habits or personal data, without their consent. It often sends this information to third parties for malicious purposes.
- **ROOTKITS-** It is a type of malware designed to gain unauthorized access to a computer system and maintain privileged control over it.
- **SOCIAL ENGINEERING IN MALWARE**- A type of malware that relies on manipulating or deceiving individuals into revealing sensitive information, such as login credentials or personal data. This malware often employs tactics such as phishing, pretexting, or baiting to trick victims into performing malicious actions.

HACKERS AND ATTACKS

TRADITIONAL HACKERS

- Motivated by thrill, validation of skills, and a sense of power.

ANATOMY OF HACK

- **RECONNAISSANCE PROBES**
  - IP Address scans to identify possible victims.
  - Port scans to learn which services are open on each potential victim host
- **THE EXPLOIT**

- The specific attack method that the attacker uses to break into the computer.

- **IP ADDRESS SPOOFING**
  - Use IP address spoofing to conceal their identities
  - Hiding the attacker's identity

EXPERT ATTACKERS - A type of hacker who possesses advanced skills, deep knowledge, and extensive experience in the field of hacking and cybersecurity.

SCRIPTS- Small programs or sets of instructions that can automate tasks. They are also used for writing viruses and other malicious software, allowing attackers to automate attacks, exploit vulnerabilities, and execute harmful actions without the user's knowledge.

SCRIPTS KIDDIE- A person who uses pre-written scripts or tools created by others to carry out cyberattacks. They typically lack advanced technical knowledge and rely on these scripts to exploit vulnerabilities, often without understanding how the attacks actually work.

CRIMINAL ERA

FRAUD - It refers to when an attacker deceives the victim into doing something against the victim's financial self-interest.

CLICK FRAUD- It is when a person or bot pretends to be a legitimate visitor on a webpage and clicks on an ad, button, or some other type of hyperlink.

FINANCIAL AND INTELLECTUAL PROPERTY THEFT- Steal money or intellectual property that they can sell to other criminals or competitors.

EXTORTION- It refers to a threat when a perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest.

STEALING SENSITIVE DATA ABOUT CUSTOMERS AND EMPLOYEES

- Carding (credit card number theft)
- Bank account theft
- Online stock account theft
- Identity theft
  - Steal enough identity information to represent the victim in large transactions, such as buying a car or even a house.

COMPETITOR THREATS

COMMERCIAL ESPIONAGE- The act of spying or stealing trade secrets, business plans, or other confidential information from a company for competitive advantage. This is usually done to gain unauthorized access to valuable business data to harm the targeted company or benefit the attacker's own business.

TRADE SECRET THEFT- The unauthorized acquisition or disclosure of a company's confidential business information, such as formulas, processes, or strategies, that gives it a competitive edge. This theft is typically done to gain a financial advantage or disrupt the targeted business.

NATIONAL INTELLIGENCE AGENCIES ENGAGE IN COMMERCIAL ESPIONAGE- Some national intelligence agencies may be involved in commercial espionage, where they gather or steal trade secrets and business information from companies of other countries. The goal is often to support national interests, such as boosting the economy, gaining a competitive edge in

industries, or undermining the economic stability of a rival nation.

CYBERWARE AND CYBERTERROR

CYBERWAR- It is refers to the use of cyberattacks which involves the use of digital means like hacking to disrupt, damage, or manipulate another nation's computer system, networks, or digital infrastructure.

CYBERTERROR- The use of cyberattacks by individuals or groups to create fear, disruption, or damage on a large scale. These attacks are typically aimed at critical infrastructure, such as power plants, transportation systems, or communication networks, with the intention of causing widespread panic, economic damage, or loss of life.

WEEK 3

PLANNING AND SECURITY

MANAGEMENT PROCESS

- Management is the hard part
- Technology is concrete
- Management, by contrast, is abstract. You cannot show pictures of devices or discuss detailed diagrams or software algorithms.

COMPREHENSIVE SECURITY -A holistic approach to protecting systems, networks, and data from various threats by implementing multiple layers of defense. This includes physical security, network security, application security, and data protection, as well as policies, procedures, and user awareness to ensure that all potential vulnerabilities are addressed.

PLAN-PROTECT-RESPOND CYCLE

PLANNING- The cycle begins with planning. Without an excellent plan, you will never have comprehensive security. Once plans are implemented, the results will feed back into planning.

PROTECTION- Protection is the plan-based creation and operation of countermeasures.

RESPOND

- Response is recovery according to plan.
- Response is complex because incidents vary in severity (and because different levels of attack severity require different response approaches.
- If response is not carefully planned in advance, it will take too long and be only partially effective.

VISION IN PLANNING

VISION- Your understanding of your role with respect to your company, its employees, and the outside world drives everything else.

SECURITY AS AN ENABLER - Your understanding about your role with respect for your company, its employees, and the outside world drives everything else.

POSITIVE VISION OF USERS

- Must not view users as malicious or stupid
- Stupid means poorly trained, and that is security's fault
- Must have zero tolerance for negative views of users

SHOULD NOT VIEW SECURITY AS POLICE OR MILITARY FORCE

- Creates a negative view of users
- Police merely punish; do not prevent crime; security must prevent attacks

- The military can use fatal force; security cannot even punish (HR does that)

CURRENT IT SECURITY GAPS

- **DRIVING FORCES**
  - The threat environment
  - Compliance laws and regulations
  - Corporate structure changes, such as mergers
- **RESOURCES**
  - Enumerate all resources
  - Rate each by sensitivity
- **DEVELOP REMEDIATION PLANS**
  - Develop a remediation plan for all security gaps
  - Develop a remediation plan for every resource unless it is well protected
- **DEVELOP AN INVESTMENT PORTFOLIO**
  - You cannot close all gaps immediately
  - Choose projects that will provide the largest returns
  - Implement these

COMPLIANCE LAWS AND REGULATIONS

Compliance laws and regulations create requirements for corporate security

- Documentation requirements are strong
- Identity management requirements tend to be strong

Sarbanes–Oxley Act of 2002 (SOX) – A U.S. law aimed at protecting investors by ensuring accurate financial reporting and requiring companies to establish strong internal controls to prevent fraud.

Privacy Protection Laws – Laws that protect personal data, like the **EU Data Protection Directive** for data privacy in the EU and the **U.S. HIPAA** for safeguarding health information.

Data Breach Notification Laws – California's SB 1386 – A law requiring businesses to notify individuals if their data is breached, setting a standard for data breach notifications in the U.S.

Federal Trade Commission (FTC) – A U.S. agency that can penalize companies for failing to protect private information, imposing fines and requiring external audits for several years to ensure compliance.

Industry Accreditation – A certification process for industries like healthcare, where organizations must meet specific security standards to be accredited, ensuring they protect sensitive information and maintain high levels of security.

PCI-DSS (Payment Card Industry Data Security Standards) – A set of security standards that applies to all businesses that accept credit cards, ensuring they protect cardholder data and maintain secure payment systems.

FISMA (Federal Information Security Management Act of 2002) – A U.S. law that establishes processes for securing information systems used by federal agencies and their contractors, ensuring the protection of sensitive government data.

ORAGANIZATION

Chief Security Officer (CSO) – The person in charge of an organization's overall security, including information and physical security. Sometimes called the **Chief Information Security Officer (CISO.)**

Where to locate IT security?

- **Within IT (In-house IT Security Team)**
  - IT security is managed by the IT department or an in-house security team that is directly integrated into the organization's technology infrastructure.
  Advantages
  • Direct Control
  • Alignment with IT Strategy
  • Customization

- **Outside IT (Dedicated External Security Team or Outsourced)**
- IT security is often handled by an external team or service provider, typically through Managed Security Service Providers (MSSPs) or third-party consultants.
  Advantages:
  •Expertise
  •Scalability
  •Focus
- **Hybrid Model (Combination of In-House and Outsourced Security)**
  -A hybrid approach combines internal and external security resources, where the in-house IT team manages day-to-day operations and works alongside external security vendors for specialized expertise, threat intelligence, or monitoring.
  Advantages:
  • Best of Both Worlds
  • Flexibility
  • Expert Support for Critical Tasks
- **Outsourcing IT Security**
  -Only e-mail or web service, Managed security service providers (MSSPs)
  • Independence from even IT security
  • MSSPs have expertise and practice-based expertise
  • Usually do not get control over policies and planning

WEEK 4

PLANNING AND SECURITY -2

RISK ANALYSIS

- The goal is a reasonable risk
- Risk analysis weighs the probable cost of compromises against the costs of countermeasures.
- Also, security has negative side effects that must be weighed
- Reasonable Risk
  - refers to the level of risk that an organization is willing to accept based on the balance between the likelihood of a threat occurring and the potential impact on the business, operations, or data.

CLASSIC RISK ANALYSIS CALCULATIONS

ASSET VALUE- THE VALUE OF THE ASSET TO BE PROTECTED.

EXPOSURE FACTOR- THE EXPOSURE FACTOR IS THE PERCENTAGE OF THE ASSET'S VALUE THAT WOULD BE LOST IN A BREACH.

SINGLE LOSS EXPECTANCY- THE SINGLE LOSS EXPECTANCY IS THE AMOUNT OF DAMAGE THAT WOULD BE SUSTAINED IN A SINGLE BREACH.

ANNUALIZED PROBABILITY OF ACCURRENCE- HOW MUCH DAMAGE

WOULD RESULT FROM A SINGLE BREACH THIS NORMALLY IS DONE ON AN ANNUALIZED BASIS.

ANNUALIZED LOSS EXPECTANCY- THE ANNUALIZED PROBABILITY OF OCCURRENCE TIMES THE SINGLE LOSS EXPECTANCY. THE YEARLY AVERAGE LOSS EXPECTED FROM THIS TYPE OF COMPROMISE FOR THIS ASSET.

COUNTERMEASURE IMPACT- THE BENEFITS OF A COUNTERMEASURE

ANNUALIZED COUNTERMEASURE COST AND NET VALUE- AVERAGE COUNTERMEASURE COST AND NET VALUE.

RESPONDING TO RISK

RISK REDUCTION- The most obvious response to risk – Adopting active countermeasures, such as installing firewalls.

RISK ACCEPTANCE- implementing no countermeasures and absorbing any damages that occur.

RISK TRANSFERENCE (INSURANCE)- having someone else absorb the risk. The most common example of risk transference is insurance.

RISK AVOIDANCE- not taking an action that is too risky.

TECHNICAL SECURITY ARCHITECTURE

- All of the company's technical countermeasures and how countermeasures are organized into a complete system of protection.

Architectural Decisions- It must be well planned to provide strong security with few weaknesses.

Dealing with Legacy Technologies-

- Technologies put in place previously
- Too expensive to upgrade all legacy technologies immediately
- Must upgrade if it seriously impairs security
- Upgrades must justify their costs

Defense in depth - A security strategy that uses multiple layers of protection to safeguard an organization's systems and data. If one layer fails, additional layers continue to provide security.

Defense in Depth vs. Weakest Links –

- **Defense in Depth**: A security approach that uses multiple layers of protection to safeguard systems, ensuring that if one layer is compromised, others can still protect the system.

- **Weakest Links**: Refers to the vulnerabilities or elements in a system that are most susceptible to attack. Even with strong defenses, if a single "weakest link" is exploited, the entire system can be compromised.

Avoiding single points of vulnerability-

• Failure at a single point can have drastic consequences
•DNS servers, central security management servers, etc.

Minimizing security burdens-

• Realistic goals

•Cannot change a company's protection level overnight • Mature as quickly as possible.

PRINCIPLES

Elements of a Technical Security Architecture -
• Border management
• Internal site management
• Management of remote connections
• Interorganizational systems with other firms
• Centralized security management
• Increases the speed of actions
• Reduces the cost of actions

POLICY-DRIVEN IMPLEMENTATION

Policies – General statements outlining what should be done, not how to do it. They provide clarity, direction, and flexibility for implementation and can vary in length.

Tiers of Security Policies - The top level is a brief corporate security policy that sets overall security goals. Below that are detailed policies covering specific areas, such as email security, hiring and firing, and protecting personally identifiable information (PII), ensuring consistent security practices across the organization.

Acceptable Use Policy – A document that outlines important rules and guidelines for users regarding the proper use of an organization's resources, often requiring users to sign for acknowledgment.

Policies for Specific Countermeasures – Policies that define security goals and outline the necessary countermeasures, while leaving the implementation details to be handled separately.

Writing Policies – Important policies require a collaborative approach, with teams including IT security, management, and legal departments. This ensures the policies have authority, cover all perspectives, and prevent errors due to IT security's limited viewpoint.

IMPLEMENTATION GUIDELINES

Implementation Guidance – Provides clear instructions to limit the discretion of implementers, simplifying decisions and preventing misinterpretation or poor choices when applying policies.

No Guidance – The implementer is solely guided by the policy, without additional instructions or support for interpreting or applying it

Standards versus Guidelines
• **Standards** are mandatory directives
• **Guidelines** are not mandatory, but must be considered

~HINDI KO NA LAGAy iba gbkjadf

WEEK 5-6

CRYPTOGRAPHY

Cryptology
- The science of encryption which encompasses cryptography and cryptanalysis.
- It refers to the study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them.

Cryptography
- The process of making and using codes to secure the transmission of information.
- Cryptography is the science of secret writing to keep the data secret, and is an important aspect

when dealing with network security. “Crypto” means secret or hidden.

- Cryptography comes from the Greek words kryptos, meaning “hidden,” and graphein, meaning “to write,” and involves making and using codes to secure messages.

Type of Cryptography

1. **Symmetric key cryptography**
   - It involves usage of one (1) secret key along with encryption and decryption algorithms which help in securing the contents of the message.
   - The strength of symmetric key cryptography depends on the number of key bits.
   - It is relatively faster than asymmetric key cryptography.
2. **Asymmetric key cryptography**
   - Also known as “public key cryptography,” it involves the usage of a public key along with the secret key.
   - It solves the problem of key distribution as both parties use different keys for encryption or decryption.
   - It is not feasible to use for decrypting bulk messages for it is very slow compared to symmetric key cryptography.
3. **Hashing**

- It involves taking the plain text and converting it to a hash value of fixed size by a hash function.
- This process ensures the integrity of the message; the hash value on both the sender’s and the receiver’s side should match if the message is unaltered.

Cryptanalysis

- The process of obtaining the plaintext message from a ciphertext message without knowing the keys used to perform the encryption.
- It involves cracking or breaking encrypted messages back into their unencrypted origins.
- For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key, or the algorithm used to encrypt it.

Types of Attacks in Cryptanalysis

1. **Classical Attack-** It can be divided into mathematical analysis and brute force attacks.
2. **Social Engineering Attack** – It is something dependent on the human factor. Tricking someone into revealing their passwords to an attacker or allowing access to a restricted area falls under this attack. People should be cautious when revealing their passwords to any third party they don't trust.
3. **Implementation Attacks-** A side-channel analysis can be used to obtain a secret key for this kind of attack. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

Classical Encryption Techniques

Caesar Cipher

- It is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is shifted to a

certain number of places down the alphabet.

Keyword Ciphers

- To use this method for constructing the ciphertext alphabet, pick a keyword and write it down while ignoring the repeated letters. Follow it with the letters of the alphabet that have not yet been used.

Giovanni's Method

- Around 1580, Giovanni Battista Argenti suggested that one can also pick a key letter and begin the keyword UNDER that letter of the plaintext.
- Around 1580, Giovanni Battista Argenti suggested that one can also pick a key letter and begin the keyword UNDER that letter of the plaintext.

Transposition Techniques

- A transposition cipher is achieved by performing some permutation on the plaintext letters.
- The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Polyalphabetic Ciphers

- Another way to improve on the simple monoalphabetic techniques is to use different monoalphabetic substitutions as one proceeds through the plaintext message.
- The best-known and simplest algorithm is referred to as the Vigenere cipher.