📘 Week 3 - Planning and Security+

Security is a process, not a product

Management Processes

- Management is the hard part
- One reason why people tend to focus on technology is that it is easier to think about technology than about management.
- Technology Is Concrete: Can visualize devices and transmission lines.
- Can understand device and software operation.
- Management, by contrast, is abstract. You cannot show pictures of devices or talk in terms of detailed diagrams or software algorithms.

Comprehensive Security

- A third reason why security management is difficult is that companies need to protect a large number of resources.
- If the failure of a single element of a system will ruin security, this is a weakest-link failure.

Plan-Protect-Respond Cycle

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.

Protection

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

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.

Vision in Planning

Vision

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

Security as an Enabler

- Security is often thought of as a preventer
- But security is also an enabler
- If a firm has good security, can do things otherwise impossible
    - Engage in interorganizational systems with other firms
    - Can use SNMP Set commands to manage their systems remotely
- Must get in early on projects to reduce inconvenience

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
- 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

General

- Documentation requirements are strong
- Identity management requirements tend to be strong
- Compliance laws and regulations create requirements for corporate security
- There are many compliance laws and regulations, and the number is increasing rapidly
- Compliance can be expensive

Examples

- Sarbanes–Oxley Act of 2002
- The European Union (EU) Data Protection Directive of 2002
- The U.S. Health Information Portability and Accountability Act (HIPAA)

Data Breach Notification Laws

- California's SB 1386
- Can punish companies that fail to protect private information
- Fines and required external auditing for several years

Federal Trade Commission

- For hospitals, etc.
- Often have accredited security requirements

Industry Accreditation

- Payment Card Industry–Data Security Standards (PCI-DSS)

FISMA

- Federal Information Security Management Act of 2002

Organization

Chief Security Officer (CSO)

Where to locate IT security?

Within IT (In-House IT Security Team)

- Direct Control
- Alignment with IT Strategy
- Customization

Outside IT (Dedicated External Security Team or Outsourced)

- Expertise
- Scalability
- Focus

Hybrid Model

- Best of Both Worlds
- Flexibility
- Expert Support for Critical Tasks

Top Management Support

- Budget
- Support in conflicts
- Setting personal examples

Relationships with Other Departments

- Special relationships
- Human resources, Legal, Auditing departments, Facilities Management

Outsourcing IT Security

- Only e-mail or webservice
- Managed security service providers (MSSPs)
- MSSPs have expertise and practice-based expertise

📘 **Week 4 - Planning and Security**

Risk Analysis

- Goal is reasonable risk
- Risk analysis weights 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 OCCURRENCE** - 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** - The yearly average countermeasure cost and net value.

Responding to Risk

- **Risk Reduction** – adopting active countermeasures such as installing firewalls
- **Risk Acceptance** – implementing no countermeasures and absorbing any damages that occur
- **Risk Transference** – having someone else absorb the risk, e.g. insurance
- **Risk Avoidance** – not taking an action that is too risky

---

Technical Security Architecture

Definition

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

Architectural Decisions

- Must be well planned to provide strong security with few weaknesses

Dealing with Legacy Technologies

- Too expensive to upgrade all legacy technologies immediately
- Must upgrade if seriously impairs security
- Upgrades must justify their costs

Principles

Defense in depth

- Resource is guarded by several countermeasures in series
- Attacker must breach them all, in series, to succeed
- If one countermeasure fails, the resource remains safe

Defense in depth versus weakest links

- Defense in depth: multiple independent countermeasures
- Weakest link: single countermeasure with multiple interdependent components

Avoiding single points of vulnerability

- Failure at a single point can have drastic consequences

Minimizing security burdens

- Realistic goals
- Cannot change a company's protection level overnight
- Mature as quickly as possible

Elements of a Technical Security Architecture

- Border management
- Internal site management
- Management of remote connections
- Interorganizational systems with other firms
- Centralized security management

Policy-driven implementation

Policies

- Statements of what is to be done
- Not in detail how it is to be done
- Allow the best possible implementation at any time

Tiers of Security Policies

- Brief corporate security policy
- Major policies (E-mail, hiring/firing, PII)
- Acceptable use policy – must be signed by users
- Policies for specific countermeasures

Writing Policies

- Policy-writing teams: IT security, department management, legal
- Team approach gives authority and avoids mistakes

Implementation Guidelines

Implementation Guidance

- Limits discretion of implementers

No Guidance

- Implementer is only guided by policy

Standards vs. Guidelines

- Standards = mandatory
- Guidelines = not mandatory

Types of Implementation Guidance

- Procedures: detailed how-to
- Segregation of duties: two people required for sensitive tasks

Request/authorization control

- Limit who may make or authorize requests
- Authorizer must never be requester

Mandatory vacations / Job rotation

- Uncover schemes requiring constant maintenance

Processes

- Less detailed than procedures; used in managerial contexts

Baselines

- Checklists of what should be done

Best practices / Recommended practices

Accountability

- Owner of resource is accountable
- Implementation can be delegated, but accountability cannot

Unclassified Information

Unclassified is **a designation to mark information that does not have potential to damage national security**

DoD unclassified data:

- Must be cleared before being released to the public
- May require application of Controlled Unclassified Information (CUI) access and distribution controls
- Must be clearly marked as Unclassified of CUI if included in a classified document or classified storage area
- If aggregated, the classification of the information may be elevated to a higher level of sensitivity or even become classified
- If compromised, could affect the safety of government personnel, missions and systems

---

CUI

Controlled Unclassified Information is **government information that must be handled using safeguarding** or **dissemination controls**. It includes, but not limited to, Controlled Technical Information (CTI), Personally Identifiable Information (PII), Protected Health Information (PHI), Financial Information, Personal or Payroll Information, and Operational Information.

It may contain information:

- Provided by a confidential source (person, commercial business or foreign government) on condition it would not be released
- Related to contractor proprietary or source selection data
- That could compromise government missions or interests

CUI is **NOT classified information** and may only be marked as CUI if belongs to a category established in the DoD CUI Registry.

Protecting PII / PHI

- Avoid storing CUI, including PII in shared folders or shared applications unless access controls are established that allow only those personnel with an official need-to-know to access the information
- Follow your organization's policies on the use of mobile computing devices and encryption
- Use only mobile devices approved by your organization
- Encrypt all CUI, including PII on mobile devices and when e-mailed. The most commonly reported cause of PII breaches is failure to encrypt e-mail messages containing PII. The DoD requires use of two-factor authentication for access
- Only use government-furnished or government-approved equipment to process CUI, including PII
- Never allow sensitive data on non-government-issued or non-government-approved mobile devices
- Never use personal e-mail accounts for transmitting PII. PII may only be e-mailed between government e-mail accounts and must be encrypted and digitally signed when possible

---

Protecting Classified Data

- Only use classified data in areas with security appropriate to classification level
- Store classified data appropriately in GSA-approved vault/container when not in use
- Don't assume open storage in a secure facility is authorized
- Weight need-to-share against need-to-know
- Ensure proper labeling:
  A. Appropriately mark all classified material and when required, unclassified and Controlled Unclassified Information (CUI) material
  B. Report inappropriately marked material
- Never transmit classified information using an unapproved method such as via an unsecure fax machine or personal mobile device

---

Spillage

Spillage **occurs when information is "spilled" from a higher classification or protection level to a lower classification** or protection level. Spillage can be either inadvertent or intentional.

To prevent inadvertent spillage:

- Always check to make sure you are using the correct network for the level of data
- Do NOT use a classified network for unclassified work. Processing unclassified information on a classified network:
  A. Can unnecessarily consume mission-essential bandwidth
  B. May illegally shield information from disclosure under the Freedom of Information Act (FOIA)
  C. Creates a danger of spillage when attempting to remove the information to an unclassified media or hard copy
- Be aware of classification markings and all handling caveats
- Follow procedures for transferring data to and from outside agency and non-Government networks, including referring vendors making solicitations to appropriate personnel
- Label all files, removable media, and subject headers with appropriate classification markings

Never use or modify government equipment for an unauthorized purpose:

- Such use or modification could be illegal
- Misuse of equipment could have a significant mission impact
- Unauthorized connection to the Internet or other network could introduce malware or facilitate hacking of sensitive or even classified information
- Any unauthorized connection creates a high potential for spillage

Never cross classification boundaries! Do not remove equipment, including mobile devices, from a

classified network for use on an unclassified network or a classified network of lower classification, or vice- versa, even if the device's memory has been purged. Never connect any unauthorized device to any network.

Marking SCI

When handling SCI:

- Mark classified information appropriately
  A. Use proper markings, including paragraph portion markings
  B. Use Security Classification Guides
  C. Use Classification Management Tool (CMT) (ICS 500-8) for email and electronic documents
- Attach appropriate cover sheets
- Take precautions when transporting classified information through unclassified areas
- Complete annually required classification training

A Security Classification Guide:

- Provides precise, comprehensive guidance regarding specific program, system, operation, or weapon system elements of information to be classified, including:
  A. Classification levels
  B. Reasons for classification
  C. Duration of classification
- approved and signed by the cognizant Original Classification Authority (OCA)
- Is an authoritative source for derivative classification
- Ensures consistent application of classification to the same information

---

Transmitting SCI

Use proper protections for transmitting and transporting SCI, such as proper wrapping and courier requirements. Dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued by the Director of National Intelligence

Printing:

- Retrieve classified documents promptly from printers
- Use appropriate classification cover sheets
- Ensure classified material is not mixed in with unclassified material being removed from SCIF
- Cover or place classified documents in a container even in an open storage environment

Fax:

- Mark SCI documents appropriately
- Send SCI information using an approved SCI fax machine
- Follow SCI handling and storage policies and procedures
- Immediately report security incidents to your Security POC

Courier:

- Authorization to escort, courier, or hand-carry SCI shall be in accordance with appropriate organization policy (agency-specific resources external to the course)
- Follow SCI transporting badge requirements and procedures
- Only transport SCI information if you have been courier-briefed for SCI
- Refer to agency-specific policies and requirements prior to transporting SCI information
- Contact your Special Security Office (SSO) or Security POC for questions/clarification

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 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

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 upon the number of key bits.
- It is relatively faster than asymmetric key cryptography.

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.

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

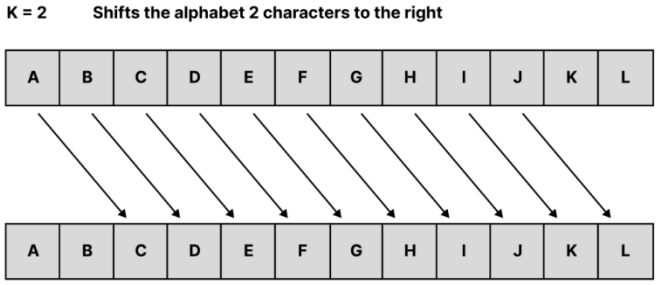
- The process of obtaining the plaintext message from a ciphertext message without knowing the keys used to perform the encryption.
- It involves cracking or breaking encrypted messages back into their unencrypted origins.
- For example, cryptanalysts seek to decrypt cipher texts without knowledge of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

TYPES OF ATTACKS IN CRYPTANALYSIS

- **Classical Attack** – It can be divided into mathematical analysis and brute force attacks.
    - **Brute force attacks** run the encryption algorithm for all possible cases of the keys until these find a match. The encryption algorithm is treated as a black box.
    - **Analytical attacks** are those attacks which focus on breaking the cryptosystem by analyzing the internal structure of the encryption algorithm.
- **Social Engineering Attack** – It is something dependent on the human factor. Tricking someone into revealing their passwords to the attacker or allowing access to the restricted area comes under this attack.
- **Implementation Attacks** – A side-channel analysis can be used to obtain a secret key for this kind of attack.

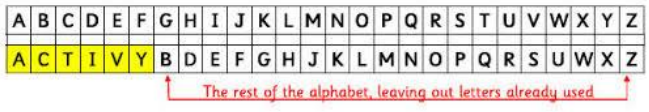
Caesar Cipher

- 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.
- For example, with a shift of 1, A would be replaced by B, B would become C, and so on.
- This method is named after Julius Caesar who used to communicate with his generals



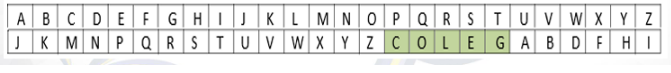
Keyword Ciphers

- 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.
- For example, find the alphabet pairs for the keyword COLLEGE. Crossing out the letters that are making their second appearance leaves COLEG. To encipher, use the pair of alphabets.



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. Method
- To use Giovanni's method with key letter "P," start the word "COLEG" under "PQRST" then place the remaining letters to the right to convert the plaintext to ciphertext.



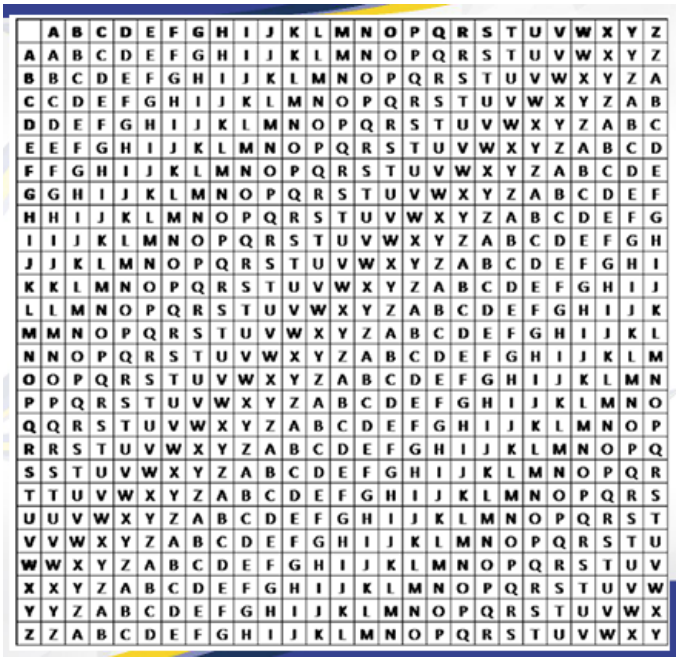
Transposition Techniques

- A transposition cipher is archived 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.

M		E		M		A		T		R		H		T		G		P		R		Y
	E		T		E		F		E		T		E		O		A		A		T	

Polyalphabetic Ciphers

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



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y