Welcome to the Fifth Chapter.

➢ Domain 5: What we will be covering.

- This is **everything** we do in our day-to-day jobs to make sure we are secure.

- Configuration, patch, and change management.
- Cryptography and hashing.
- Attacks on our cryptography.
- Data handling, classification, labeling, retention, and destruction/disposal.
- Administrative (Directive) controls.
- Security awareness training.
- Social engineering.

Configuration Management:

- **Configuration Management:**
  - When we receive or build new systems, they often are completely open, before we introduce them to our environment we harden them.
  - We develop a long list of ports to close, services to disable, accounts to delete, missing patches and many other things.
  - Often it is easier to have OS images that are completely hardened and use the image for the new system, we then update the image when new vulnerabilities are found or patches need to be applied, often though we use a standard image and just apply the missing patches.
  - We do this for any device on our network, servers, workstations, phones, routers, switches,...
  - Pre-introduction into our production environment we run vulnerability scans against the system to ensure we didn't miss anything (Rarely done on workstations, should be done on servers/network equipment).
  - Having a standard hardening baseline for each OS ensures all servers are similarly hardened and there should be no weak links, we also have the standardized hardening making troubleshooting much easier.
  - Once a system is introduced to our production environment we monitor changes away from our security baseline, most changes are administrators troubleshooting or making workarounds, which may or may not be allowed, but it could also be an attacker punching a path out of our network.

Patch Management:

- **Patch Management:**
  - In order to keep our network secure we need to apply patches on a regular basis.
  - Whenever a vulnerability is discovered the software producer should release a patch to fix it.
  - Most organizations give the patches a few weeks to be reviewed and then implement them in their environment.

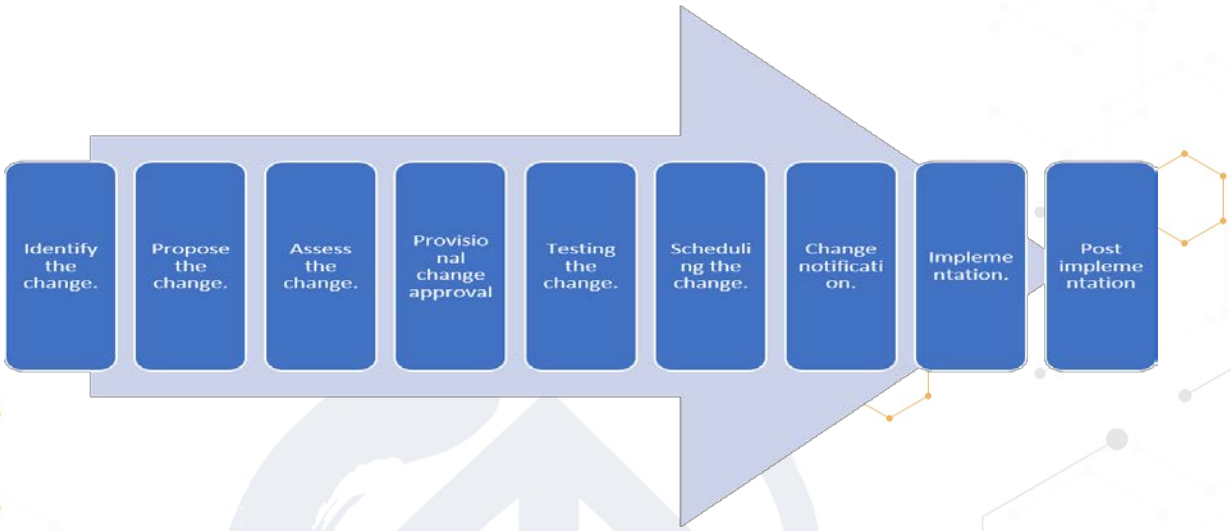
- We normally remember the OS patches, but can often forget about network equipment updates, array updates, IoT updates and so on, if they are not patched, we are not fully using defense in depth and we can expose ourselves to risk.
- We use software to push our patches to all appropriate systems, this is easier, we ensure all systems gets patched and they all get the same parts of the patch, we may exclude some parts that have an adverse effect on our network.

Change Management:

- **Change Management:**
  - Our formalized process on how we handle changes to our environments.
  - If done right we will have full documentation, understanding and we communicate changes to appropriate parties.
  - The change review board should be comprised of both IT and other operational units from the organization, we may consider impacts on IT, but we are there to serve the organization, they need to understand how it will impact them and raise concerns if they have any.
  - A change is proposed to the change board, they research in order to understand the full impact of the change.
  - The person or group submitting the change should clearly explain the reasons for the change, the pro's and con's of implementing and not implementing, any changes to systems and processes they know about and in general aide and support the board with as much information as needed.
  - The board can have senior leadership on it or they can have a predefined range of changes they can approve and anything above that threshold they would make recommendations but changes require senior leadership approval.

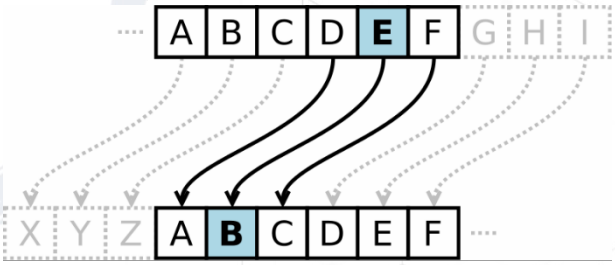
  - There are many different models and process flows for change management, some are dependent on organization structure, maturity, field of business and many other factors.
    * A generalized flow would look like this:
      → Identifying the change.
      → Propose the change.
      → Assessing risks.
      → Provisional change approval.
      → Testing the change.
      → Scheduling the change.
      → Change notification for impacted parties.
      → Implementing the change.
      → Post implementation reporting of the actual change impact.

- We closely monitor and audit changes, remember changes can hold residual risk which we would then have to mitigate.
- Everything in the change control process should be documented and kept, often auditors want to see that we have implemented proper change controls, and that we actually follow the paper process we have presented them with.



Cryptography:

- **The History of Cryptography** (yes, this is testable).
  - **Spartan Scytale** - Message written lengthwise on a long thin piece of parchment wrapped around a certain size round stick. By itself it would make no sense, but if rewrapped around a stick of the same diameter it would be decipherable.
  - **Caesar Cipher** (Substitution) - Done by switching Letters by a certain number of spots in the alphabet.



- For the exam, what you need to know is that cryptography helps us:
  - Keep our secrets secret (**Confidentiality**) ← This is what most people think all cryptography does.
  - Keep our data unaltered (**Integrity**).
  - Provide a way to verify (**Authentication**) our Subjects; it can also provide **non-repudiation**.

- **Definitions:**
  - **Cryptology** is the science of securing communications.
  - **Cryptography** creates messages where the meaning is hidden.
  - **Cryptanalysis** is the science of breaking encrypted communication.

    - Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.
    - It uses mathematical analysis of the cryptographic algorithm, as well as side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation and the devices that run them.
  - **Cipher** is a cryptographic algorithm.
  - **Plaintext** (Cleartext) is an unencrypted message.
  - **Ciphertext** is an encrypted message.
  - **Encryption** converts the plaintext to a ciphertext.
  - **Decryption** turns a ciphertext back into a plaintext.
  - **Book Cipher** - Use of a well-known text (Often a book) as the key.
    - Messages would then look like 244.2.13, 12.3.7, 41.42.1,...
    - The person reviewing the message would look at page 244, sentence 2, word 13, then page 12, sentence 3, word 7, page 41, sentence 42 word 1,...
  - **Running-Key Cipher** – uses a well-known test as a key as well but uses a previously agreed upon phrase.
    - The sender would add the plaintext message to the letters from the key, and the receiver would subtract the letters from the key.

- **Asymmetric vs Symmetric Encryption and Hybrid:**
  - **Asymmetric**
    - Pros: It does not need a pre-shared key, only 2x users = total keys.
    - Cons: It is much slower; it is weaker per bit.
  - **Symmetric**:
    - Pros: Much faster, stronger per bit.
    - Cons: Needs a pre-shared key, **n(n-1)/2** users, becomes unmanageable with many users.

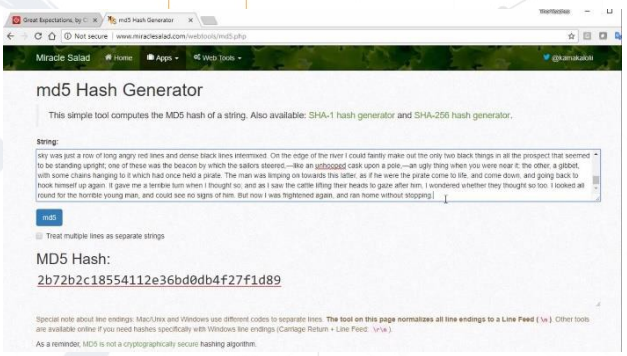
Users	Symmetric keys	Asymmetric Keys
2	1	4
5	10	10
10	45	20
30	435	60
100	4,950	200
500	124,750	1000
5000	12,497,500	10000
10000	49,995,000	20000

- **Asymmetric Encryption (Public Key Encryption):**
  - **Asymmetric Encryption uses 2 keys: A Public Key and a Private Key (Key Pair):**
    - Your **Public Key** is publicly available.
      - → Used by others to encrypt messages sent to you. Since the key is asymmetric, the cipher text can't be decrypted with your public Key.
    - Your **Private Key** - You keep this safe.
      - → You use it to decrypt messages sent with your public key.

- **Asymmetric vs Symmetric Encryption and Hybrid:**
  - **Hybrid Encryption:**
    - Uses Asymmetric encryption to share a Symmetric Key (session key).
    - We use the security over an unsecure media from Asymmetric for the initial exchange and we use the speed and higher security of the Symmetric for the actual data transfer.
    - The Asymmetric Encryption may send a new session key every so often to ensure security.

Hashing:

- **Hash Functions** (One-Way Hash Functions) are used for **Integrity**:
  - A **variable-length plaintext** is hashed into a **fixed-length value** hash or MD (Message Digest).
  - It is used to prove the Integrity of the data has not changed. Even changing a comma in a 1000-page document will produce an entirely new hash.
  - **Collisions:** When 2 hashes of different data provide the same hash. It is possible, but very unlikely.
  - Just 1 bit change completely changes the hash.
  - Using Great Expectations (Charles Dickens 1867 Edition again, 4 pages at font size 11, 1827 words, 7731 characters).
  - **Hash#1** is the original **2b72b2c18554112e36bd0db4f27f1d89**
  - **Hash#2** is with 1 comma removed **21b78d32ed57a684e7702b4a30363161**
  - Just a single "." added will change the hash value to **5058f1af8388633f609cadb75a75dc9d**

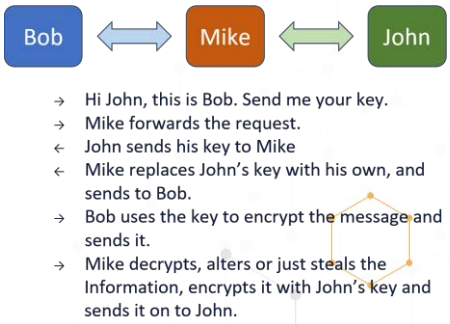


Attacks on our Cryptography:

- **Cryptographic Attacks:**
  - **Steal the Key:** Modern encryption being so difficult to break, it is easier to recover the private key.
    - Law enforcement does this when they get search warrants, to recover the private key from the PC or phone of someone charged with a crime.
    - Attackers do this by gaining access to your system or key repository; they can then decrypt your data.
  - **Brute Force:**
    - Uses the entire key space (every possible key); with enough time, any plaintext can be decrypted.
    - Effective against all key-based ciphers except the one-time pad; it would eventually decrypt it, but it would also generate so many false positives that the data would be useless.

- **Key stretching:** Adding 1-2 seconds to password verification.
  - If an attacker is brute forcing password and needs millions of attempts, it will become an unfeasible attack vector.

- **Man-in-the-Middle Attack (MITM):**
  - The attacker secretly relays and may alter communication between two parties, who believe they are directly communicating with each other.
  - The attacker must be able to intercept all relevant messages passing between the two victims.
  - They can alter the information, just steal it or inject new messages.



- **Side Channel Attacks:**
  - Attackers use physical data to break a crypto system. This can be CPU cycles, power consumption while encrypting/decrypting,...

Data Handling Classification Labeling Retention Destruction/Disposal:

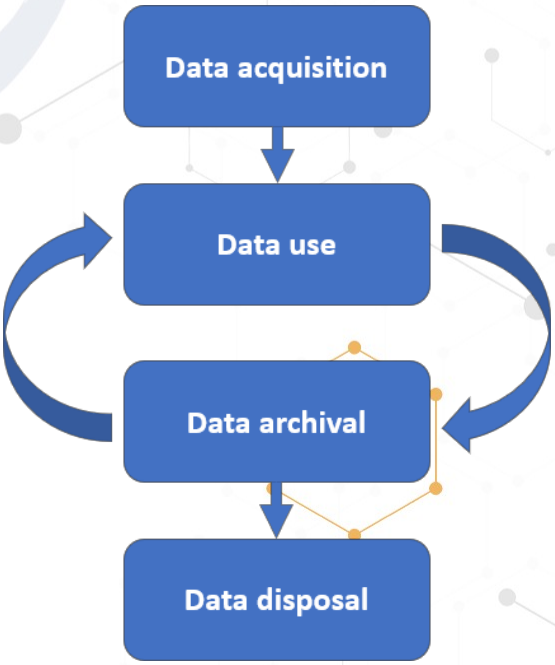
- **Sensitive information**
  - **Data handling:**
    - Only trusted individuals should handle our data; we should also have policies on how, where, when, and why the data was handled. Logs should be in place to show these metrics.
  - **Data storage:**
    - Where do we keep our sensitive data? It should be kept in a secure, climate-controlled facility, preferably geographically distant or at least far enough away that potential incidents will not affect that facility too.
    - Many older breaches were from bad policies around tape backups.
    - Tapes were kept at the homes of employees instead of at a proper storage facility or in a storage room with no access logs and no access restrictions (often unencrypted).
  - **Data retention:**
    - Data should not be kept beyond the period of usefulness or beyond the legal requirements (whichever is greater).
    - Regulation (HIPAA or PCI-DSS) may require a certain retention of the data (1, 3, 7 years, or infinity).
    - Each industry has its own regulations and company policies may differ from the statutory requirements.
    - Know your retention requirements!

- **Paper disposal** – It is highly encouraged to dispose of ANY paper with any data on it in a secure manner. This also has standards and cross shredding is recommended.
  It is easy to scan and have a program re-assemble documents from normal shreds like this one.

- **Digital disposal** – The digital disposal procedures are determined by the type of media.
  - **Deleting, formatting, and overwriting (Soft destruction):**
    - **Deleting** a file just removes it from the table; everything is still recoverable.
    - **Formatting** does the same, but it also puts a new file structure over the old one. Still recoverable in most cases.
    - **Overwriting** (Clear) is done by writing 0s or random characters over the data.
    - **Sanitization** is a process of rendering target data on the media infeasible for a given level of recovery effort.
    - **Purge** is removing sensitive data from a system or device to a point where data recovery is no longer feasible even in a laboratory environment.

- **Degaussing** destroys magnetic media by exposing it to a very strong magnetic field. This will also most likely destroy the media integrity.
- **Full physical destruction is safer than soft destruction:**
  - **Disk crushers** do exactly what their name implies: they crush disks (often used on spinning disks).
  - **Shredders** do the same thing as paper shredders do; they just work on metal. These are rare to have at normal organizations, but you can buy the service.
  - **Incineration, pulverizing, melting, and acid** are also (very rarely) used to ensure full data destruction.
- It is common to do multiple types of data destruction on sensitive data (both degaussing and disk crushing/shredding).

- **The Information Life Cycle:**
  - **Data acquisition.**
    - The information is either created or copied from another location.
    - Make it useful, index it, and store it.
  - **Data use.**
    - How to we ensure the data is kept confidential, the integrity is intact, and it is available when needed (The CIA triad).
  - **Data archival.**
    - Retention required by law, or the data will be used later.
  - Archival vs. backup.
  - **Data disposal.**
    - How do we dispose properly of the data once it is no longer useful and required.

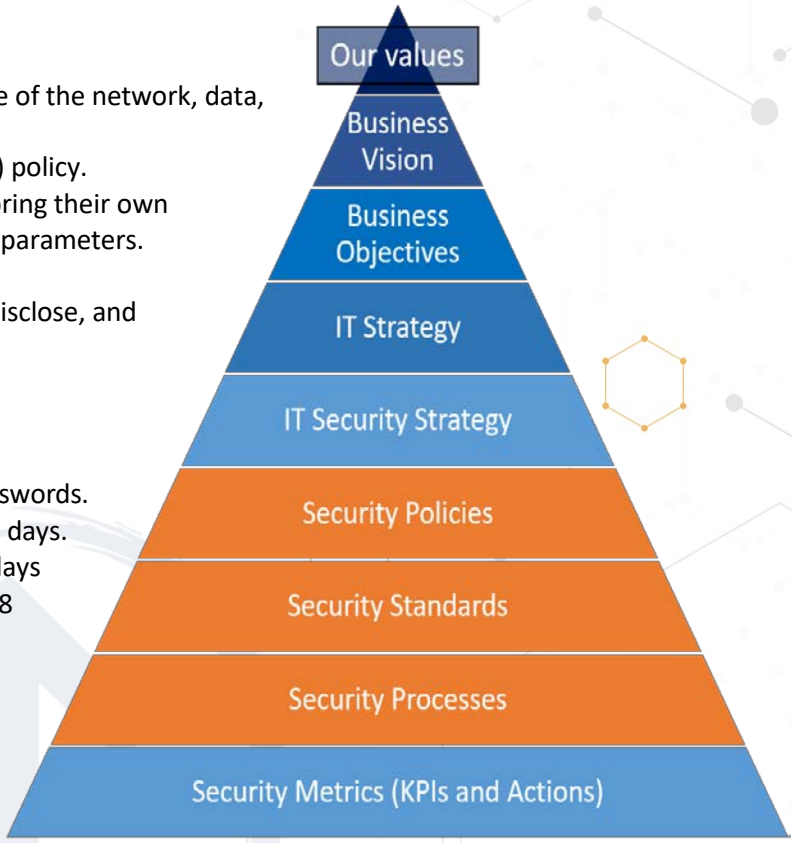


Administrative (Directive) Controls:

- **Access Control Categories:**
  - **Administrative (Directive) Controls:**
    - Organizational policies and procedures.
  - **Technical Controls:**
    - Hardware/software/firmware – Firewalls, routers, encryption.
  - **Physical Controls:**
    - Locks, fences, guards, dogs, gates, bollards.

- **Access Control Types:**
  - **Access Control Types** (Many can be multiple types – On the exam look at question content to see which type it is).
    - **Preventative:**
      - → Prevents action from happening.
    - **Detective:**
      - → Controls that Detect during or after an attack.
    - **Corrective:**
      - → Controls that Correct an attack.
    - **Recovery:**
      - → Controls that help us Recover after an attack.
    - **Deterrent:**
      - → Controls that Deter an attack.
    - **Compensating:**
      - → Controls that Compensate.

- **Policies – Mandatory and high level.**
  - **AUP** (Acceptable Use Policy).
    - What is acceptable use of the network, data, resources, …
  - **BYOD** (Bring Your Own Device) policy.
    - Allows employees to bring their own devices within certain parameters.
  - **Privacy policy.**
    - How we gather, use, disclose, and manage private data.



- **Policies – Mandatory.**
  - **Password policy.**
    - Remember last 24 passwords.
    - Max. password age 90 days.
    - Min. password age 2 days
    - Min. password length 8 characters.
    - Complex passwords.
    - Stored not using reversible encryption.
  - , …

- **Data handling policy:**
- Classify, categorize, label, encrypt, store, backup, disposal/destroy.

- **Data has 3 States:**
  - **Data at Rest:** Stored data.
  - **Data in Motion:** Data being transferred on a network.
  - **Data in Use:** We are actively using the files/data, it cannot be encrypted.

Training and Awareness:

- **Users often pose the largest security risk:**
  - **Training:** Provides users with a skillset - this is nice, but if they ignore the knowledge, it does nothing.
  - **Awareness**: Change user behavior - this is what we want, we want them to change their behavior.
  - We want to build a cybersecurity culture, with a good cyber hygiene.

Social Engineering:

- **Cryptographic Attacks:**
  - **Social Engineering:**
    - Much easier than breaking the key is convincing the key holder to hand it over to the “help desk”.

FREE ICE CREAM!

- A very successful social engineering attack was a Pentest company driving up in front of a company office with "Free Ice Cream” and company logo signs on an ice cream van.

- **Social Engineering** uses people skills to bypass security controls.
  - Can be used in a combination with many other attacks, especially client-side attacks or physical tests.
  - Attacks are often more successful if they use one or more of these approaches:
    - **Authority (someone you trust or are afraid of)** - Look and sound like an authority figure, be in charge, this can be in a uniform or a suit. Most effective with impersonation, whaling, and vishing attacks.
    - **Intimidation (If you don't bad thing happens)** - Virus on the network, credit card compromised, lawsuit against your company, intimidation is most effective with impersonation and vishing attacks.

- **Social Engineering Attacks:**
  - **Consensus (Following the crowd, everyone else was doing it)** - Fake reviews on a website, using consensus/social proof is most effective with Trojans and hoaxes.
  - **Scarcity (If you don't act now, it is too late)** - New iPhone out, only 200 available, often effective with phishing and Trojan attacks.
  - **Urgency (It has to happen now or else)** - The company will be sued for $1,000,000 if these papers are not filled out before Friday, often used with Phishing.
  - **Familiarity (Have a common ground or build it)** - Knowing something about the victim ahead of time and then reference it can raise chances of a successful attack drastically. People want to be helpful, if they feel like they know you they want too even more. Often successful with vishing and in-person social engineering.

- **Phishing, spear phishing, and whale phishing:** Fishing spelled in hacker speak with Ph not F.
  - **Phishing** (Social engineering email attack):
    - Click to win, Send information to get your inheritance …
    - Sent to hundreds of thousands of people; if just 0.02% follow the instructions they have 200 victims.
      - → A public treasurer in Michigan sent $1.2m to Nigeria ($1.1m of taxpayer funds and $72,000 of his own).

- **Spear Phishing:** Targeted phishing, not just random spam, but targeted at specific individuals.
  - Sent with knowledge about the target (person or company); familiarity increases success.
- **Whale Phishing (Whaling):** Spear phishing targeted at senior leadership of an organization.
  - This could be: "Your company is being sued if you don't fill out the attached documents (with trojan in them) and return them to us within 2 weeks".
- **Vishing (Voice Phishing):** Attacks over automated VOIP (Voice over IP) systems, bulk spam similar to phishing.
  - These are: "Your taxes are due", "Your account is locked" or "Enter your PII to prevent this" types of calls.

➢ Domain 5: What we covered.

- This is **everything** we do in our day-to-day jobs to make sure we are secure.

- Configuration, patch, and change management.
- Cryptography and hashing.
- Attacks on our cryptography.
- Data handling, classification, labeling, retention, and destruction/disposal.
- Administrative (Directive) controls.
- Security awareness training.
- Social engineering.