Module-1

Security Policies

- An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements.

Security Policies

- What is the purpose of an information security policy?
  - An information security policy aims to enact protections and limit the distribution of data to only those with authorized access.
  - Organizations create ISPs to:
    - Establish a general approach to information security
    - Document security measures and user access control policies
    - Detect and minimize the impact of compromised information assets such as misuse of data, networks, mobile devices, computers and applications
    - Protect the reputation of the organization

Security Policies

- What is the purpose of an information security policy?
  - An information security policy aims to enact protections and limit the distribution of data to only those with authorized access.
  - Organizations create ISPs to:
    - Comply with legal and regulatory requirements like NIST, GDPR, HIPAA and FERPA
    - Protect their customer's data, such as credit card numbers
    - Provide effective mechanisms to respond to complaints and queries related to real or perceived cyber security risks such as phishing, malware and ransomware
    - Limit access to key information technology assets to those who have an acceptable use

Security Policies

- Why is an information security policy is important?
  - Creating an effective information security policy and that meets all compliance requirements is a critical step in preventing security incidents like data leaks and data breaches.
  - ISPs are important for new and established organizations.
  - Increasing digitalization means every employee is generating data and a portion of that data must be protected from unauthorized access.
  - Depending on your industry, it may even be protected by laws and regulations.

Security Policies

- Why is an information security policy is important?
  - Sensitive data, personally identifiable information (PII), and intellectual property must be protected to a higher standard than other data.
  - Whether you like it or not, information security (InfoSec) is important at every level of your organization and outside of your organization.
  - Increased outsourcing means third-party vendors have access to data too.
  - Third-party risk management and vendor risk management is part of any good ISP.
  - Third-party risk, fourth-party risk and vendor risk are equally important.

Security Policies

- What are the key elements of an information security policy?
  1. Purpose
  2. Audience
  3. Information security objectives
  4. Authority and access control policy
  5. Data classification
  6. Data support and operations
  7. Security awareness training
  8. Responsibilities and duties of employees

Security Policies

- What are the key elements of an information security policy?
  - 1. Purpose
    - Preserve your organization's information security.
    - Detect and preempt information security breaches caused by third-party vendors, misuse of networks, data, applications, computer systems and mobile devices.
    - Protect the organization's reputation
    - Uphold ethical, legal and regulatory requirements
    - Protect customer data and respond to inquiries and complaints about non-compliance of security requirements and data protection.

Security Policies

- What are the key elements of an information security policy?
  - 2. Audience
    - Define who the information security policy applies to and who it does not apply to.
    - You may be tempted to say that third-party vendors are not included as part of your information security policy.

Security Policies

- What are the key elements of an information security policy?
  - 3. Information security objectives
    - **Confidentiality:** data and information are protected from unauthorized access
    - **Integrity:** Data is intact, complete and accurate
    - **Availability:** IT systems are available when needed

Security Policies

- What are the key elements of an information security policy?
  - 4. Authority and access control policy
    - This part is about deciding who has the authority to decide what data can be shared and what can't.
    - Remember, this may not be always up to your organization.
    - For example, if you are the CSO at a hospital. You likely need to comply with HIPAA and its data protection requirements. If you store medical records, they can't be shared with an unauthorized party whether in person or online.

Security Policies

- What are the key elements of an information security policy?
  - 5. Data classification
    - An information security policy must classify data into categories. A good way to classify the data is into five levels that dictate an increasing need for protection:
      - **Level 1:** Public information
      - **Level 2:** Information your organization has chosen to keep confidential but disclosure would not cause material harm
      - **Level 3:** Information has a risk of material harm to individuals or your organization if disclosed
      - **Level 4:** Information has a high risk of causing serious harm to individuals or your organization if disclosed
      - **Level 5:** Information will cause severe harm to individuals or your organization if disclosed

Security Policies

- What are the key elements of an information security policy?
  - 6. Data support and operations
    - Once data has been classified, you need to outline how data is each level will be handled.
    - There are generally three components to this part of your information security policy:
      - **Data protection regulations:**
        - » Organizations that store personally identifiable information (PII) or sensitive data must be protected according to organizational standards, best practices, industry compliance standards and regulation
      - **Data backup requirements:**
        - » Outlines how data is backed up, what level of encryption is used and what third-party service providers are used
      - **Movement of data:**
        - » Outlines how data is communicated. Data that is deemed classified in the above data classification should be securely communicated with encryption and not transmitted across public networks to avoid man-in-the-middle attacks

Security Policies

- What are the key elements of an information security policy?
  - 7. Security awareness training
    - Security training should include:
      - **Social engineering:**
        - » Teach your employees about phishing, spearphishing and other common social engineering cyber attacks
      - **Clean desk policy:**
        - » Laptops should be taken home and documents shouldn't be left on desks at the end of the work day
      - **Acceptable usage:**
        - » What can employees use their work devices and Internet for and what is restricted?

Security Policies

- What are the key elements of an information security policy?
  - 8. Responsibilities and duties of employees
    - This is where you operationalize your information security policy. This part of your information security policy needs to outline the owners of:
      - Security programs
      - Acceptable use policies
      - Network security
      - Physical security
      - Business continuity
      - Access management
      - Security awareness
      - Risk assessments
      - Incident response
      - Data security
      - Disaster recovery
      - Incident management

Basic Terminologies in Cryptography

- Plaintext
- Ciphertext
- Encryption
- Decryption
- Keys
- Hash
- Salt
- Symmetric and Asymmetric Algorithms
- Public and Private Keys
- HTTPS
- End-to-End Encryption

Basic Terminologies in Cryptography

- Plaintext
  - which is simple but just as important as the others: **plaintext** is an unencrypted, readable, plain message that anyone can read.

Basic Terminologies in Cryptography

- **Ciphertext**
  - **Ciphertext** is the result of the encryption process.
  - The encrypted plaintext appears as apparently random strings of characters, rendering them useless.
  - A cipher is another way of referring to the encryption algorithm that transforms the plaintext, hence the term ciphertext.

Basic Terminologies in Cryptography

- **Encryption**
  - **Encryption** is the process of applying a mathematical function to a file that renders its contents unreadable and inaccessible---unless you have the decryption key.
  - For instance, let's say you have a Microsoft Word document.
  - You apply a password using Microsoft Office's inbuilt encryption function.
  - The file is now unreadable and inaccessible to anyone without the password. You can even encrypt your entire hard drive for security.

Basic Terminologies in Cryptography

- **Decryption**
  - If encryption locks the file, then decryption reverses the process, turning ciphertext back to plaintext.
  - **Decryption** requires two elements: the correct password and the corresponding decryption algorithm.

Basic Terminologies in Cryptography

- **Keys**
  - The encryption process requires a **cryptographic key** that tells the algorithm how to transform the plaintext into ciphertext.
  - **Kerckhoffs's principle** states that "only secrecy of the key provides security," while Shannon's maxim continues "the enemy knows the system."

Basic Terminologies in Cryptography

- **Keys**
  - These two statements influence the role of encryption, and keys within that.
  - Keeping the details of an entire encryption algorithm secret is extremely difficult; keeping a much smaller key secret is easier.
  - The key locks and unlocks the algorithm, allowing the encryption or decryption process to function.

Basic Terminologies in Cryptography

- **Keys**
  - **Is a Key a Password?**
    - No. Well, at least not entirely. Key creation is a result of using an algorithm, whereas a password is usually a user choice.
    - The confusion arises as we rarely specifically interact with a cryptographic key, whereas passwords are part of daily life.
    - Passwords are at times part of the key creation process. A user enters their super-strong password using all manner of characters and symbols, and the algorithm generates a key using their input.

Basic Terminologies in Cryptography

- **Hash**
  - When a website encrypts your password, it uses an encryption algorithm to convert your plaintext password to a hash.
  - A **hash** is different from encryption in that once the data is hashed, it cannot be unhashed. Or rather, it is extremely difficult.
  - Hashing is really useful when you need to verify something's authenticity, but not have it read back. In this, password hashing offers some protection against **brute-force attacks** (where the attacker tries every possible password combination).

Basic Terminologies in Cryptography

- **Hash**
  - You might have even heard of some of the common hashing algorithms, **such as MD5, SHA, SHA-1, and SHA-2**. Some are stronger than others, while some, such as MD5, are outright vulnerable.
  - For instance, if you head to the site **MD5 Online**, you'll note they have 123,255,542,234 words in their MD5 hash database.

Basic Terminologies in Cryptography

- **Salt**
  - When passwords are part of key creation, the encryption process requires additional security steps.
  - One of those steps is **salting** the passwords.
  - At a basic level, a salt adds random data to a one-way hash function.

Basic Terminologies in Cryptography

- **Salt**
  - There are two users with the exact same password: **hunter2**.
  - We run **hunter2** through an SHA256 hash generator and receive f52fbd32b2b3b86ff88ef6c490628285f482af15ddcb29541f94bcf526a3f6c7.
  - Someone hacks the password database and they check this hash; each account with the corresponding hash is immediately vulnerable.

Basic Terminologies in Cryptography

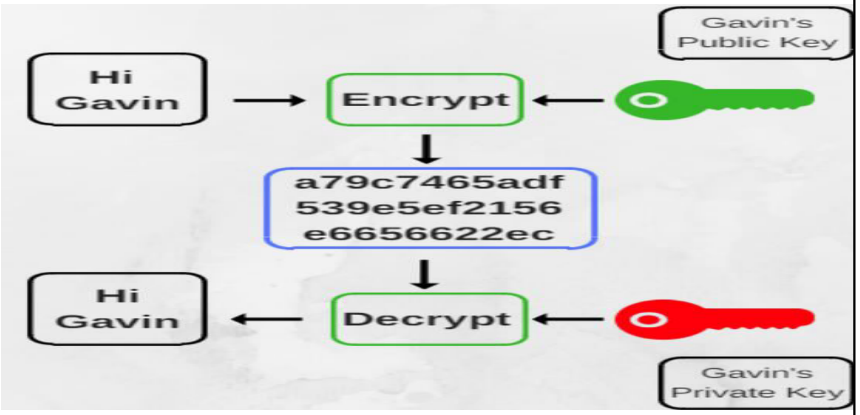
- **Symmetric and Asymmetric Algorithms**
  - In modern computing, there are two primary encryption algorithm types: symmetric and asymmetric. They both encrypt data, but function in a slightly different manner.
    - **Symmetric algorithm:**
      - Uses the same key for both encryption and decryption. Both parties must agree on the algorithm key before commencing communication.
    - **Asymmetric algorithm:**
      - Uses two different keys: a public key and a private key. This enables secure encryption while communicating without previously establishing a mutual algorithm. This is also known as **public key cryptology**

Basic Terminologies in Cryptography

- **Public and Private Keys**
  - An asymmetric algorithm uses two keys: a **public key** and a **private key**.
  - The public key can be sent to other people, while the private key is only known by the owner.
  - What's the purpose of this?
    - Well, anyone with the intended recipient's public key can encrypt a private message for them, while the recipient can only read the contents of that message provided they have access to the paired private key. Check out the below image for more clarity.

Basic Terminologies in Cryptography

- **Public and Private Keys**



Basic Terminologies in Cryptography

- **Public and Private Keys**
  - Public and private keys also play an essential role in **digital signatures**, whereby a sender can sign their message with their private encryption key.
  - Those with the public key can then verify the message, safe in the knowledge that the original message came from the sender's private key.
  - A **key pair** is the mathematically linked public and private key generated by an encryption algorithm.

Basic Terminologies in Cryptography

- **HTTPS**
  - **HTTPS (HTTP Secure)** is a now widely implemented security upgrade for the HTTP application protocol that is a foundation of the internet as we know it.
  - When using a HTTPS connection, your data is encrypted using Transport Layer Security (TLS), protecting your data while in transit.
  - HTTPS generates long-term private and public keys that in turn are used to create a short-term session key.

Basic Terminologies in Cryptography

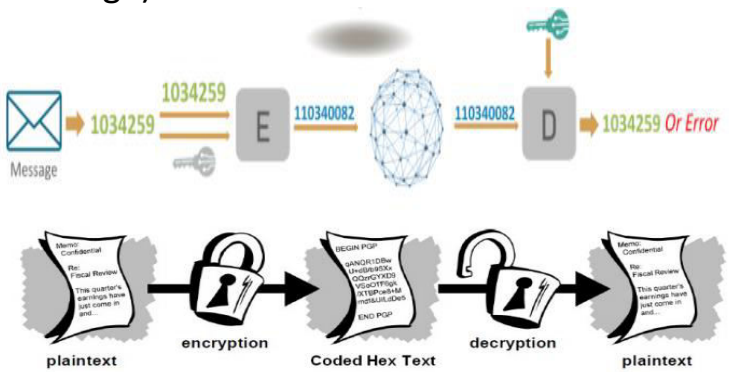
- **HTTPS**
  - The session key is a single-use symmetric key that the connection destroys once you leave the HTTPS site (closing the connection and ending its encryption).
  - However, when you revisit the site, you will receive another single-use session key to secure your communication.
  - A site must completely adhere to HTTPS to offer users complete security.
  - Since 2018 the majority of sites online began offering HTTPS connections over standard HTTP.

Basic Terminologies in Cryptography

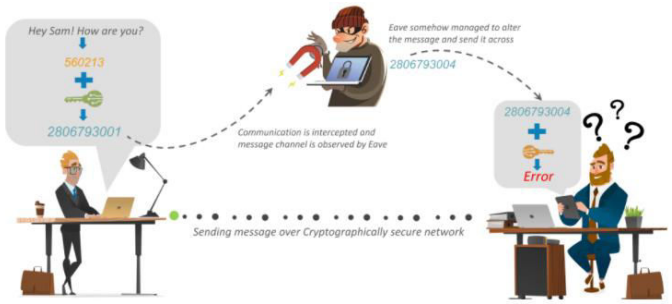
- **End-to-End Encryption**
  - One of the biggest encryption buzzwords is that of **end-to-end encryption**.
  - Social messaging platform service WhatsApp began offering its users end-to-end encryption (E2EE) in 2016, making sure their messages are private at all times.
  - WhatsApp isn't the first, or even the only **messaging service to offer end to end encryption**.
  - Idea of mobile message encryption further into the mainstream - much to the ire of myriad government agencies around the world.

Encryption (Cryptography)

- "hidden writing" (hiding the meaning of the message)



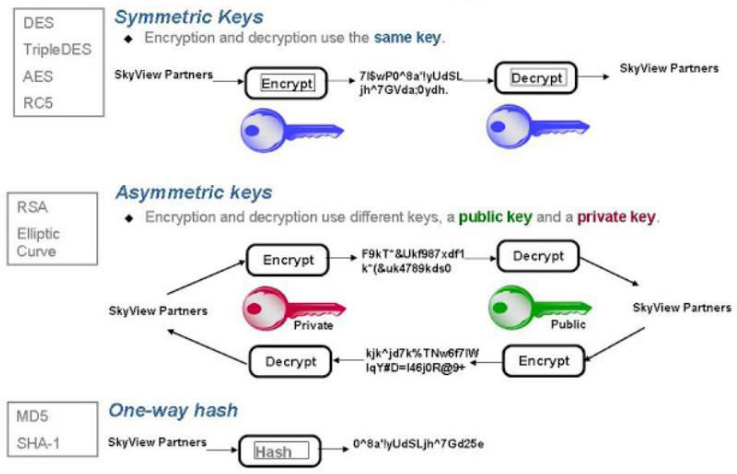
Encryption (Cryptography)



Encryption (Cryptography)

- Basic security goals:
  - privacy (secrecy, confidentiality)
    - only the intended recipient can see the communication
  - authenticity (integrity)
    - the communication is generated by the alleged sender

Types of Encryption Algorithms



Module-1

Identity and Access Management (IdAM)

- Identity and Access Management (IAM or IdAM for short) is a way to tell who a user is and what they are allowed to do.
- IAM is like the bouncer at the door of a nightclub with a list of who is allowed in, who isn't allowed in, and who is able to access the VIP area.
- IAM is also called identity management (IdM).

Identity and Access Management (IdAM)

- In more technical terms, IAM is a means of managing a given set of users' digital identities, and the privileges associated with each identity.
- Within an organization, IAM may be a single product, or it may be a combination of processes, software products, cloud services, and hardware that give administrators visibility and control over the organizational data that individual users can access.

Identity and Access Management (IdAM)

- Identity in the context of computing
  - A person's entire identity cannot be uploaded and stored in a computer, so "identity" in a computing context means a certain set of properties that can be conveniently measured and recorded digitally.
  - Think of an ID card or a passport: not every fact about a person is recorded in an ID card, but it contains enough personal characteristics that a person's identity can quickly be matched to the ID card.

Identity and Access Management (IdAM)

- Identity in the context of computing
  - To verify identity, a computer system will assess a user for characteristics that are specific to them.
  - If they match, the user's identity is confirmed. These characteristics are also known as "authentication factors,".
  - The three most widely used authentication factors are:
    - Something the user knows
    - Something the user has
    - Something the user is

Identity and Access Management (IdAM)

- Identity in the context of computing
  - Something the user has:
    - This factor refers to possession of a physical token that is issued to authorized users.
    - The most basic example of this authentication factor is the use of a physical house key to enter one's home.
    - The assumption is that only someone who owns, rents, or otherwise is allowed into the house will have a key.

Identity and Access Management (IdAM)

- Identity in the context of computing
  - Something the user is:
    - This refers to a physical property of one's body.
    - A common example of this authentication factor in action is Face ID, the feature offered by many modern smartphones.
    - Fingerprint scanning is another example.
    - Less common methods used by some high-security organizations include retina scans and blood tests.

Identity and Access Management (IdAM)

- Access management
  - "Access" refers to what data a user can see and what actions they can perform once they log in.
  - Once John logs into his email, he can see all the emails he has sent and received.
  - However, he should not be able to see the emails sent and received by Tracy, his coworker.

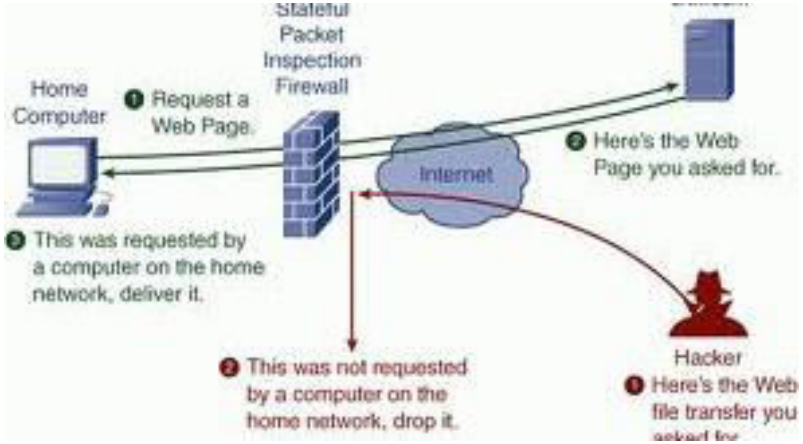
What is a Firewall?

- Hardware or software device that protects a computer network from unauthorized access.

How a Firewall works

- Firewalls filters the information coming through the Internet connection into a user private network.
- To control traffic in and out of the network firewalls one or more of the three methods are used including:
  - Packet filtering
  - Proxy service
  - Stateful inspection

Diagram of Firewall



Additional Information about Firewalls

- Most home network routers have built in firewall.
- The term "firewall" originated from firefighting, where a firewall is a barrier established to prevent the spread of a fire.
- A firewall works with the proxy server making request on behalf of workstation users.
- There are a number of features firewalls can include from logging and reporting to setting alarms of an attack.
- Costs for host based firewalls usually costs around $100 or less.
- Some may costs more depending on different things such as features included or if its an enterprise based system.

What is Ethical Hacking?

- Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network.
- The company that owns the system or network allows Cyber Security engineers to perform such activities in order to test the system's defenses.
- Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

What is Ethical Hacking?

- Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy.
- They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications.
- By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

What is Ethical Hacking?

- Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches.
- Consider it a high-tech permutation of the old saying “It takes a thief to catch a thief.”

What is Ethical Hacking?

- They check for key vulnerabilities include but are not limited to:
  - Injection attacks
  - Changes in security settings
  - Exposure of sensitive data
  - Breach in authentication protocols
  - Components used in the system or network that may be used as access points

Type of Hackers

- The practice of ethical hacking is called “White Hat” hacking, and those who perform it are called White Hat hackers.
- In contrast to Ethical Hacking, “Black Hat” hacking describes practices involving security violations.
- The Black Hat hackers use illegal techniques to compromise the system or destroy information.

White Hat vs Black Hat Hacker

- Difference between White Hat and Black Hat hackers - motives are different.
- Black Hat hackers are motivated by malicious intent, manifested by personal gains, profit, or harassment; whereas
- White Hat hackers seek out and remedy vulnerabilities, so as to prevent Black Hats from taking advantage.

Ethical Hacker Roles and Responsibilities

- An ethical hacker must seek authorization from the organization that owns the system.
- Hackers should obtain complete approval before performing any security assessment on the system or network.
- Determine the scope of their assessment and make known their plan to the organization.
- Report any security breaches and vulnerabilities found in the system or network.

Ethical Hacker Roles and Responsibilities

- Keep their discoveries confidential.
- As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement.
- Erase all traces of the hack after checking the system for any vulnerability.
- It prevents malicious hackers from entering the system through the identified loopholes.

References

- https://purplesec.us/red-team-vs-blue-team-cyber-security/
- https://purplesec.us/penetration-test/

What is Traffic?

- Traffic basically connects a computer with a web browser and an actual human being with digital content sitting on a hosting server.
- Without the former, the latter has no purpose nor value whatsoever making traffic an essential commodity for legitimate web companies and the criminal underground economy alike.
- Traffic is redirected and shuffled around the web, the visitor info of which is passed along as part of partnerships and business contracts.
- In fact, entire ecosystems and economies have developed around traffic that buy, sell, and trade it.
- Products and services have been designed and deployed to aid in analyzing and classifying it.
- Code that tracks traffic is deployed at several points along the way, usually on services no one readily sees or recognizes, each gathering their small amount of insight that can drive content to optimize the flow of traffic.
- Traffic and the insight thereof is critical to the giant exchanges in the online advertising space and the very many niche affiliate network programs that help monetize and squeeze every last fraction of a penny of indirect marginal profit out of the edges of the URL visited.
- A key commodity in the underground economy, playing an important role in malware delivery operations.

Monetizing traffic in malicious web space via traffic filtering

- Monetize traffic runs rampant across the web traffic space, from web advertisements to malicious traffic distribution feeding the latest malware variant to the un-patched masses.
- Internet attackers can cast wide nets to reach many potential victims in their campaigns.
- For instance:
  - Spam is distributed to large lists of recipients, sending malicious URLs and attachments to contacts that may have been stolen from address books, harvested from websites, collected from data breach dumps, or purchased from various sellers and marketing database suppliers.
  - Web traffic is hijacked and rerouted from thousands of compromised websites, bringing all kinds of visitors who are running various desktop operating systems and web browsers and using different types of mobile devices.
  - SEO efforts pump thousands of websites running cloned content that would never be sought out by visitors to the top of search results, drawing more clicks.
  - Traffic is outright purchased, leveraging the economy of scale of the underground to supply more volume. Some actors tap into the advertising space and the significant amount of traffic it can provide. Others seek out the bounties of web traffic from the adult publisher space and low-quality ads space supplying traffic from popups, popunders, and unintended affiliate offer clicks.
- For "traffers," or actors dealing illegally in traffic, it's a matter of separating the wheat from the chaff.
- Traffers attempting to monetize web traffic directly or to sell it to others need to be able to deliver as clean and valuable a product as possible

Filtering techniques

- It is helpful to understand the many ways in which attackers filter clients in their infrastructure.
- There are a few main reasons why filtering occurs:
  - Optimization: Making sure traffic is unique. Traffers often get paid only for unique traffic.
  - Targeting: Making sure traffic meets requirements for location, user or device type, and similar constraints.
  - Anti-analysis/anti-research: Making sure malicious traffic distribution and end-threats are not analyzed and detected by security companies or related investigators.

Traffic Filtering Techniques

- There are four basic recommendations for traffic filtering in order to reduce security threats, organisations use various devices, technologies and techniques for traffic filtering.
- Each institution/ organization that wishes to improve the efficiency of filtering and increase the level of security in its network should apply a set of recommendations (next refer slide)…

Traffic Filtering Techniques

1. **Traffic-filtering rules**
   - To determine the manner in which the incoming and outgoing traffic flows in the network are regulated.
   - A set of traffic-filtering rules can be adopted as an independent packet filtering policy or as a part of the information security policy.
2. **Select a traffic-filtering technology**
   - To be implemented depending on the requirements and needs;
3. **Implement defined rules**
   - The selected technology should optimise the performance of devices
4. **Maintain all the components of the solution**
   - Includes not only devices, but also the policy.

Firewall

- Firewalls provide critical protection for business systems and information.
- Operating according to prewritten security rules, firewalls are applications that monitor and manage the traffic flowing into and out of your network.
- Firewall types tend to be either network firewalls running on network hardware or host-based firewalls that rely on host computers to oversee traffic.
- Traffic-filtering technologies are commonly divided into
  - Stateless firewall
  - Stateful firewall
- Stateful firewalls are capable of monitoring and detecting states of all traffic on a network to track and defend based on traffic patterns and flows.
- Stateless firewalls focus on individual packets, using preset rules to filter traffic.

https://www.cdw.com/content/cdw/en/articles/security/2019/04/29/stateful-versus-stateless-firewalls.html

Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewalls have been a first line of defense in network security for over 25 years.
- They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be hardware, software, or both.

Packet-filtering functionality (stateless firewall)

- Packet filtering is the basic feature of all firewall devices.
- It is built into the majority of operating systems and devices with a traffic routing feature.
- Most of the cases, it is a router on which access control lists (ACLs) are applied.
- A packet filter implemented on a router is the simplest, but only one of the available traffic-filtering methods.

Packet-filtering functionality (stateless firewall)

- The first firewall devices, with only a packet filter, were also called stateless inspection firewalls.
- Unlike them, modern firewall devices provide far more possibilities for packet filtering.
- A packet filter enables the implementation of control of access to resources by deciding whether a packet should be allowed to pass, based on the information contained in the IP packet header.

Packet-filtering functionality (stateless firewall)

- The packet filter does not analyse the content of the packet (unlike a content filter), nor does it attempt to determine the sessions to which individual packets belong, based on the information contained in the TCP or UPD header, and therefore it does not make any further decisions in that regard.
- For this reason, the process is also known as stateless packet inspection.
- Due to its manner of operation, which does not track the information on the state of connections, it is necessary to explicitly allow two-way traffic on the connection when configuring a stateless firewall device.
- Stateless firewall devices analyse each packet individually and filter them based on the information contained in Layers 3 and 4 of the OSI reference model.

Packet-filtering functionality (stateless firewall)

- A filtering decision is made based on the following information:
  - ❖ Source IP address;
  - ❖ Destination IP address;
  - ❖ Protocol;
  - ❖ Source port number;
  - ❖ Destination port number.

They are commonly implemented as a part of the functionality on routers (ACL, firewall filters, etc.), But can also be implemented on servers

Packet-filtering functionality (stateless firewall)

- **The advantages of applying packet filters:**
  - Simplified implementation;
  - Supported by most routers, so there is no need to invest in new equipment and software;
  - Rarely cause bottlenecks in the area of their application, even at high speeds in gigabit networks.

Packet-filtering functionality (stateless firewall)

- **Disadvantages of applying packet filters:**
  - Vulnerable to IP spoofing attacks;
  - Vulnerable to attacks that exploit problems within the TCP/IP specification and the protocol stack;
  - Problems with filtering packets that are fragmented (causing interoperability and non functioning of VPN connections);
  - No support for the dynamic filtering of some services (the services that require dynamic negotiation about the ports that will be used in communication – passive FTP).

Stateful packet inspection

- It improves the packet filtering process by monitoring the state of each connection established through a firewall device.
- It is known that the TCP protocol, allows two-way communication and that TCP traffic is characterized by three phases: establishing the connection, data transfer, and terminating the connection.

Stateful packet inspection

- In the connection establishment phase, stateful packet inspection records each connection in the state-table.
- In the data transfer phase, the device monitors certain parameters in the header of the L3 packet and L4 segment and makes a filtering decision depending on their values and the content of the state-table.

Stateful packet inspection

- The state-table contains all currently active connections.
- As a result, a potential attacker trying to spoof a packet with a header indicating that the packet is a part of an established connection can only be detected by the stateful inspection firewall device, which verifies whether the connection is recorded in the state-table.

Stateful packet inspection

- The state-table contains the following information:
  - ❖Source IP address;
  - ❖Destination IP address;
  - ❖Source port number;
  - ❖Destination port number;
  - ❖TCP sequence numbers;
  - ❖TCP flag values.

Stateful packet inspection

- The state of the synchronize (SYN), reset (RST), acknowledgment (ACK) and finish (FIN) flags are monitored within the TCP header and a conclusion is reached about the state of a specific connection.
- The UDP protocol does not have a formal procedure for establishing and terminating a connection.

Stateful packet inspection

- Devices with stateful inspection can monitor the state of individual flows and match different flows when they logically correspond to each other
- E.g., A DNS response from an external server will only be allowed to pass if the corresponding DNS query from the internal source to that server has previously been recorded.

Stateful packet inspection

- **Advantages of applying stateful firewall devices:**
  - A higher level of protection compared to stateless firewall devices (greater efficiency and moredetailed traffic analysis);
  - Detection of IP spoofing and dos attacks;
  - More log information compared to packet filters.

Stateful packet inspection

- **Disadvantages of applying stateful firewall devices:**
  - No protection against application layer attacks;
  - Performance degradation of the router on which they are deployed (this depends on the size of the network and other services run on the router);
  - Not all of them provide support for UDP, GRE and IPSEC protocols, treating them in the same way as stateless firewall devices;
  - No support for user authentication.

What is a next-generation firewall?

- A traditional firewall provides stateful inspection of network traffic.
- A next-generation firewall (NGFW) allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.
- In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks.
- A next-generation firewall (NGFW) is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS).
- Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection and third-party identity management integration (i.e. LDAP, RADIUS, Active Directory).
- NGFWs use a more thorough inspection style, checking packet payloads and matching signatures for harmful activities such as exploitable attacks and malware

What is a next-generation firewall?

- According to Gartner's definition, a next-generation firewall must include:
  - Standard firewall capabilities like stateful inspection
  - Integrated intrusion prevention
  - Application awareness and control to see and block risky apps
  - Threat intelligence sources
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats

What should I look for in a next-generation firewall?

1. Breach prevention and advanced security
2. Comprehensive network visibility
3. Flexible management and deployment options
4. Fastest time to detection
5. Automation and product integrations

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html#

Threat-focused NGFW

- These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation.
- With a threat-focused NGFW you can:
  - Know which assets are most at risk with complete context awareness
  - Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
  - Better detect evasive or suspicious activity with network and endpoint event correlation
  - Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
  - Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

Unified threat management (UTM) firewall

- A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus.
- It may also include additional services and often cloud management.
- UTMs focus on simplicity and ease of use.

Proxy firewalls

- Proxy firewalls filter network traffic at the application level.
- Unlike basic firewalls, the proxy acts an intermediary between two end systems.
- The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked.
- Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic.

Network address translation (NAT) firewalls

- Network address translation (NAT) firewalls allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden.
- As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks.
- NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

Stateful multilayer inspection (SMLI) firewalls

- SMLI firewalls filter packets at the network, transport, and application layers, comparing them against known trusted packets.
- Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually.
- These firewalls examine packets to determine the state of the communication to ensure all initiated communication is only taking place with trusted sources.

Pros of Stateless Firewalls	Cons of Stateless Firewalls
+ Stateless firewalls deliver fast performance.	– Stateless firewalls do not inspect traffic.
+ Heavy traffic is no match for stateless firewalls, which perform well under pressure without getting caught up in the details.	– The stateless firewall also does not examine an entire packet, but instead decides whether the packet satisfies existing security rules.
+ Stateless firewalls have historically been cheaper to purchase, although these days stateful firewalls have significantly come down in price.	– These firewalls require some configuration to arrive at a suitable level of protection.

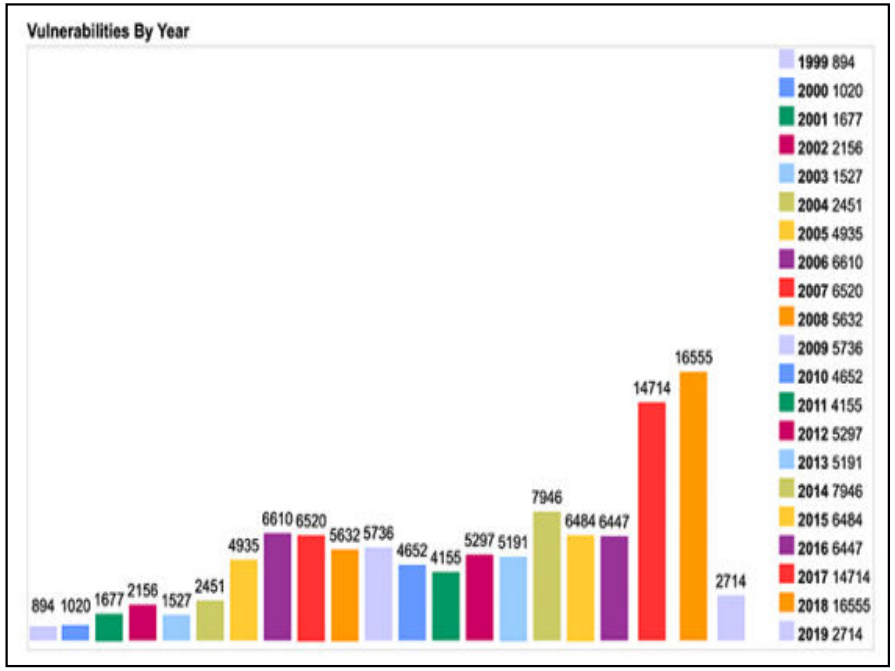
Pros of Stateful Firewalls	Cons of Stateful Firewalls
+ Stateful firewalls are highly skilled at detecting unauthorized attempts or forged messaging.	– Vulnerabilities may allow a hacker to compromise and take control over a firewall that is not updated with the latest software releases.
+ The powerful memory retains key attributes of network connections.	– Some stateful firewalls can be tricked to allow or even attract outside connections with an action as simple as viewing a webpage.
+ These firewalls do not need many ports open for proper communication.	– Man-in-the-middle attacks may pose greater vulnerabilities.
+ Stateful firewalls offer extensive logging capabilities and robust attack prevention.	
+ An intelligent system, stateful firewalls base future filtering decisions on the cumulative sum of past and present findings.	

Module-2

System Security

Module-2: System Security

- System Vulnerabilities
- Network Security Systems
- System Security & System Security Tools
- Web Security
- Application Security
- Intrusion Detection Systems



System Vulnerabilities

- **Vulnerabilities** are weaknesses in a system that gives threats the opportunity to compromise assets.
- All systems have vulnerabilities.
- Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc.

System Vulnerabilities

- Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.
  1. **Hardware Vulnerability**
  2. **Software Vulnerability**
  3. **Network Vulnerability**
  4. **Procedural Vulnerability**

System Vulnerabilities

1. **Hardware Vulnerability**
   - A hardware vulnerability is a weakness which can be used to attack the system hardware through physically or remotely.
   - For example:
     - Old version of systems or devices
     - Unprotected storage
     - Unencrypted devices, etc

System Vulnerabilities

2. Software Vulnerability:

- A software error happen in development or configuration such as the execution of it can violate the security policy.
- For example:
  - Lack of input validation
  - Unverified uploads
  - Cross-site scripting
  - Unencrypted data, etc.

System Vulnerabilities

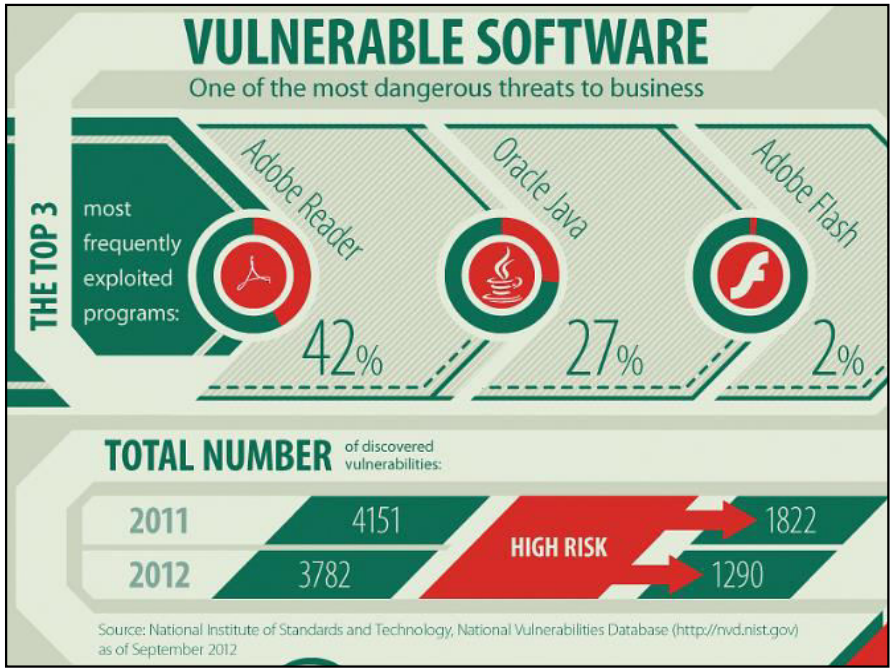
3. Network Vulnerability:

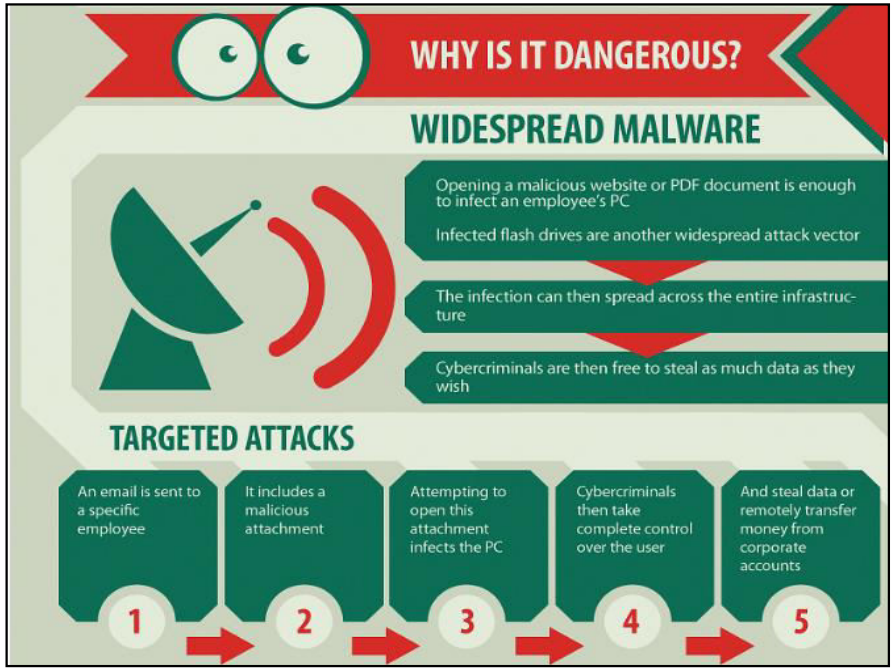
- A weakness happen in network which can be hardware or software.
- For example:
  - Unprotected communication
  - Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
  - Social engineering attacks
  - Misconfigured firewalls

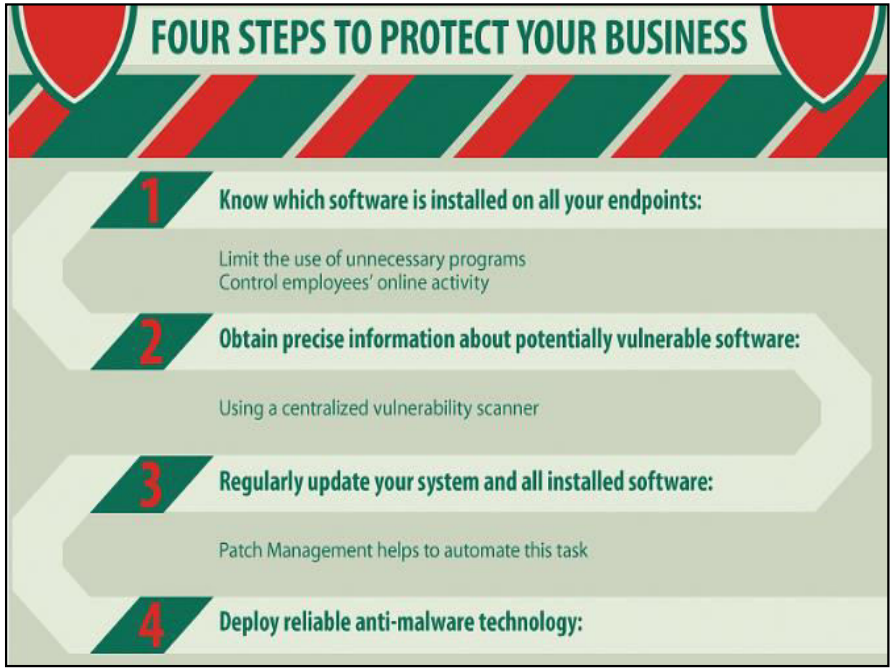
System Vulnerabilities

4. Procedural Vulnerability:

- A weakness happen in an organization operational methods.
- For example:
  - Password procedure – Password should follow the standard password policy.
  - Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.







System Vulnerabilities

- OS-based vulnerabilities
  - **1. Remote code execution**
  - **2. Denial-of-service**
  - **3. Elevation of privilege**
  - **4. Information disclosure**
  - **5. Spoofing**

System Vulnerabilities

- OS-based vulnerabilities
  - **1. Remote code execution**
    - Remote code execution, also known as RCE, is a type of vulnerability that allows attackers to remotely run arbitrary code on vulnerable servers and workstations.
    - Attackers can then perform actions to exploit other vul nerabilities.
    - Remote code execution is the most common vulnerability found in software today, and it can lead to other attacks, including denial-of-service and elevation of privileges.

System Vulnerabilities

- OS-based vulnerabilities
  - **2. Denial-of-service**
    - Denial-of Service (DoS) is one of the major Microsoft STRIDE threats that make services like Windows and browsers unable to function regularly .
    - There are two types of DoS vulnerabilities:
      - a. Flood attacks
      - b. Crash attacks

System Vulnerabilities

- OS-based vulnerabilities
  - **3. Elevation of privilege**
    - Elevation of privilege, also known as privilege escalation or EoP, gives an attacker authorization permissions beyond those initially granted.
    - In an EoP attack, a remote user executes commands to give an unauthorized user the rights of an administrator.

System Vulnerabilities

- OS-based vulnerabilities
  - **4. Information disclosure**
    - You've likely heard about the recent data breaches through wh ich hackers captured the personal information of several top government officials.
    - This type of attack, information disclosure, occurs when software bugs are exploited to obtain personal data stored in a computer's memory.
    - Even when this personal data isn't used in an immediate attack, this data can serve as a key building block for a future cyberattack.

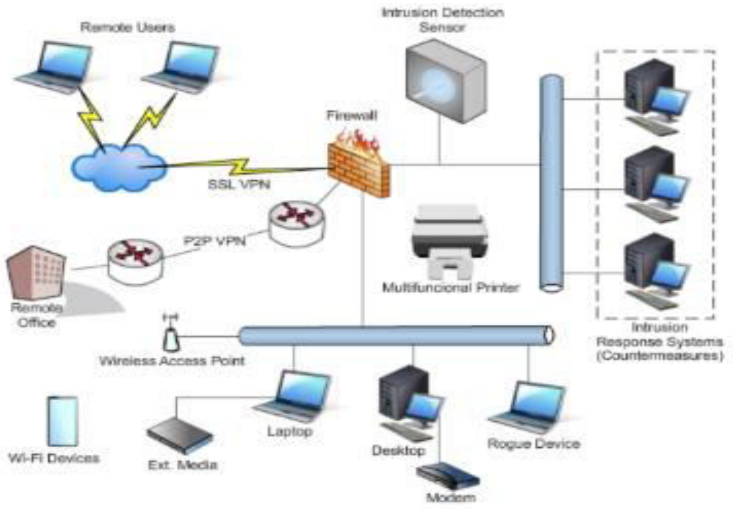
System Vulnerabilities

- OS-based vulnerabilities
  - **5. Spoofing**
    - Spoofing is the process of impersonating someone by tampering with the authentication process using a username and password.
    - Hackers can use spoofing to access personal information in a victim's account.
    - Spoofing mostly occurs in applications that use the Chakra scripting engine, such as Microsoft's Internet Explorer and Edge.

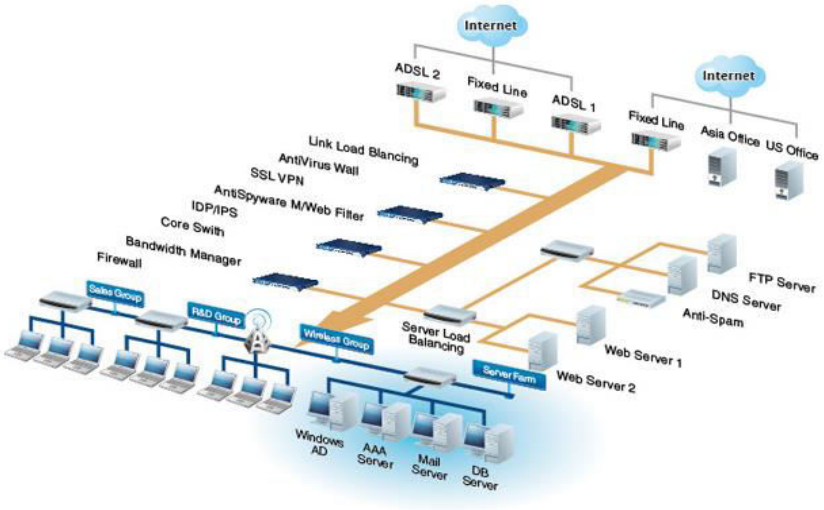
System Vulnerabilities

- The most common software security vulnerabilities include:
  - Missing data encryption
  - OS command injection
  - SQL injection
  - Buffer overflow
  - Missing authentication for critical function
  - Missing authorization
  - Unrestricted upload of dangerous file types
  - Reliance on untrusted inputs in a security decision
  - Cross-site scripting and forgery
  - Download of codes without integrity checks
  - Use of broken algorithms
  - URL redirection to untrusted sites
  - Path traversal
  - Bugs
  - Weak passwords
  - Software that is already infected with virus

Network Security Systems



Network Security Systems



Network Security Systems

- It is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.
- Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Network Security Systems

- How does network security work?
  - There are many layers to consider when addressing network security across an organization.
  - Attacks can happen at any layer in the network security layers model, so your network security hardware, software and policies must be designed to address each area.
  - Network security typically consists of three different controls: physical, technical and administrative.

Network Security Systems

- **Physical Network Security**
  - Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on.
  - Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

Network Security Systems

- **Technical Network Security**
  - Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network.
  - Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Network Security Systems

- **Administrative Network Security**
  - Administrative security controls consist of security policies and processes that control user behaviour, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

References

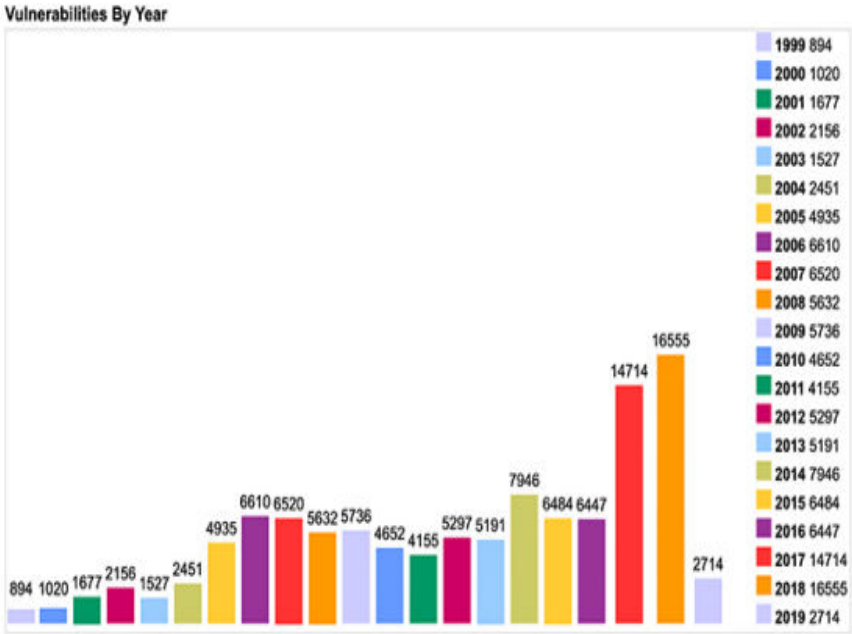
- https://www.kaspersky.co.in/resource-center/threats/malware-system-vulnerability
- https://inside.battelle.org/blog-details/hardware-vs.-software-vulnerabilities
- https://whatis.techtarget.com/definition/hardware-vulnerability
- https://www.perforce.com/blog/kw/common-software-vulnerabilities
- https://purplesec.us/network-vulnerability/
- https://www.redteamsecure.com/blog/the-most-common-types-of-network-vulnerabilities

Module-2

System Security

Module-2: System Security

- System Vulnerabilities
- Network Security Systems
- System Security & System Security Tools
- Web Security
- Application Security
- Intrusion Detection Systems



System Vulnerabilities

- **Vulnerabilities** are weaknesses in a system that gives threats the opportunity to compromise assets.
- All systems have vulnerabilities.
- Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc.

System Vulnerabilities

- Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.
  1. **Hardware Vulnerability**
  2. **Software Vulnerability**
  3. **Network Vulnerability**
  4. **Procedural Vulnerability**

System Vulnerabilities

1. Hardware Vulnerability

– A hardware vulnerability is a weakness which can be used to attack the system hardware through physically or remotely.

– For example:
  - Old version of systems or devices
  - Unprotected storage
  - Unencrypted devices, etc

System Vulnerabilities

2. Software Vulnerability:

– A software error happen in development or configuration such as the execution of it can violate the security policy.

– For example:
  - Lack of input validation
  - Unverified uploads
  - Cross-site scripting
  - Unencrypted data, etc.

System Vulnerabilities

3. Network Vulnerability:

- A weakness happen in network which can be hardware or software.

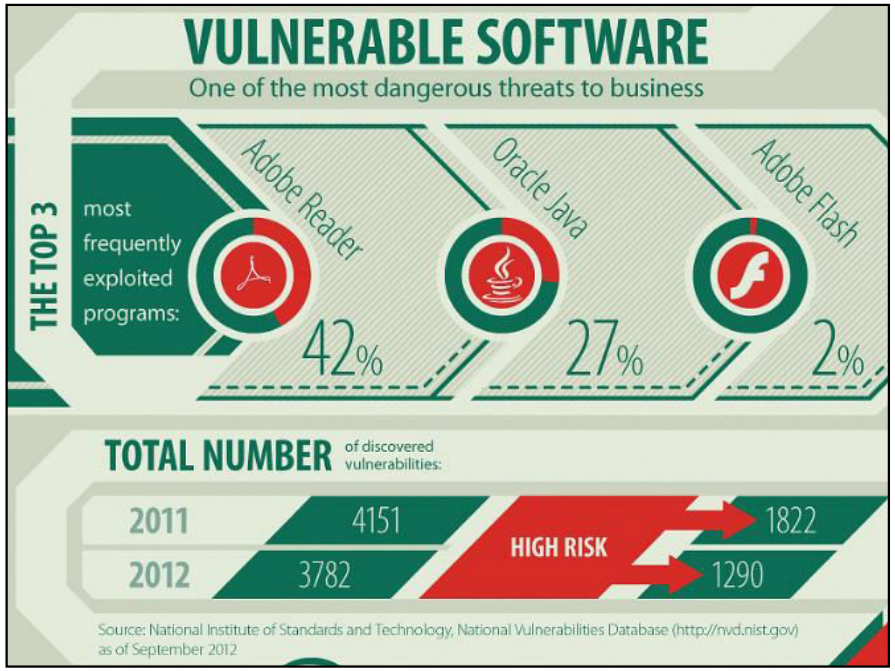
- For example:
  - Unprotected communication
  - Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
  - Social engineering attacks
  - Misconfigured firewalls

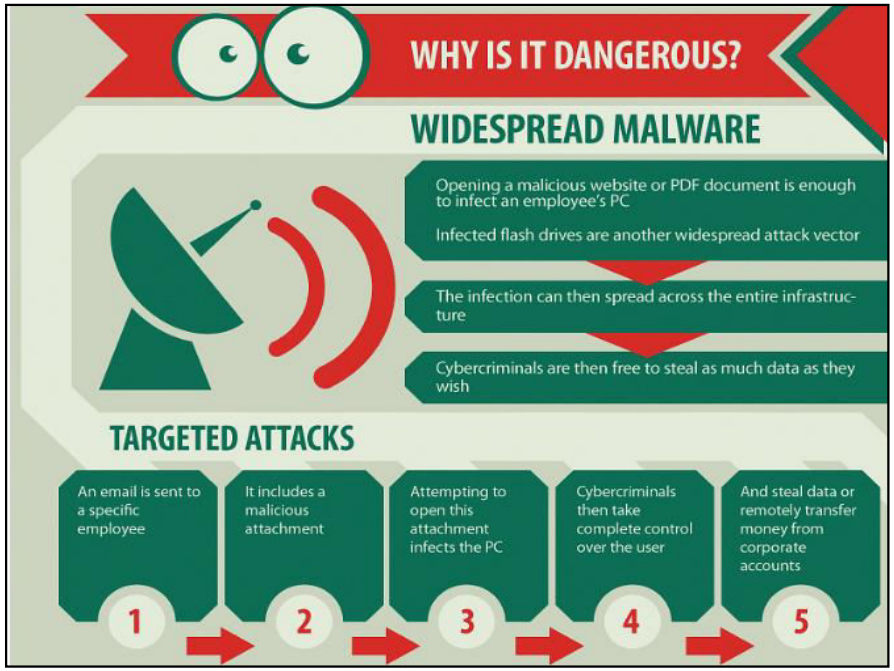
System Vulnerabilities

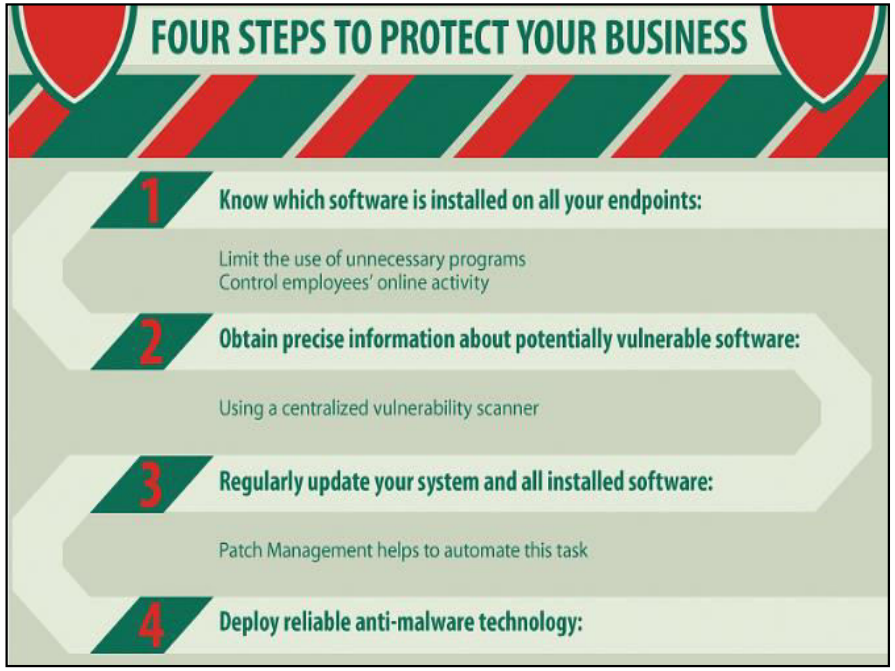
4. Procedural Vulnerability:

- A weakness happen in an organization operational methods.

- For example:
  - Password procedure – Password should follow the standard password policy.
  - Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.







System Vulnerabilities

- OS-based vulnerabilities
  - **1. Remote code execution**
  - **2. Denial-of-service**
  - **3. Elevation of privilege**
  - **4. Information disclosure**
  - **5. Spoofing**

System Vulnerabilities

- OS-based vulnerabilities
  - **1. Remote code execution**
    - Remote code execution, also known as RCE, is a type of vulnerability that allows attackers to remotely run arbitrary code on vulnerable servers and workstations.
    - Attackers can then perform actions to exploit other vul nerabilities.
    - Remote code execution is the most common vulnerability found in software today, and it can lead to other attacks, including denial-of-service and elevation of privileges.

System Vulnerabilities

- OS-based vulnerabilities
  - **2. Denial-of-service**
    - Denial-of Service (DoS) is one of the major Microsoft STRIDE threats that make services like Windows and browsers unable to function regularly .
    - There are two types of DoS vulnerabilities:
      - a. Flood attacks
      - b. Crash attacks

System Vulnerabilities

- OS-based vulnerabilities
  - **3. Elevation of privilege**
    - Elevation of privilege, also known as privilege escalation or EoP, gives an attacker authorization permissions beyond those initially granted.
    - In an EoP attack, a remote user executes commands to give an unauthorized user the rights of an administrator.

System Vulnerabilities

- OS-based vulnerabilities
  - **4. Information disclosure**
    - You've likely heard about the recent data breaches through wh ich hackers captured the personal information of several top government officials.
    - This type of attack, information disclosure, occurs when software bugs are exploited to obtain personal data stored in a computer's memory.
    - Even when this personal data isn't used in an immediate attack, this data can serve as a key building block for a future cyberattack.

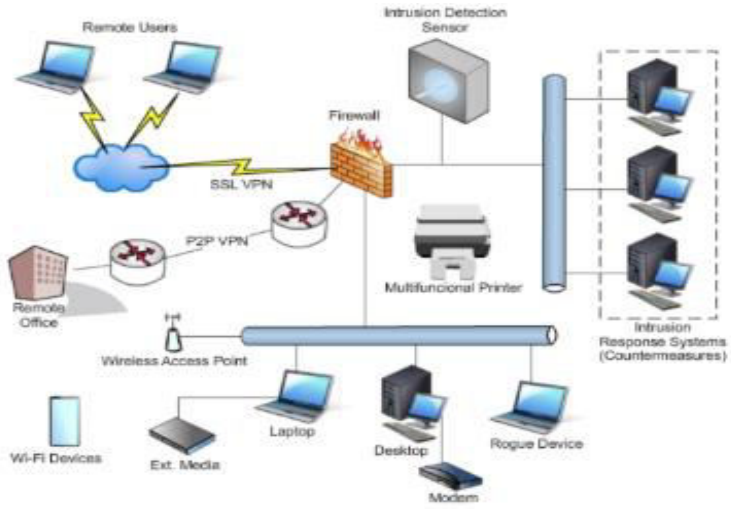
System Vulnerabilities

- OS-based vulnerabilities
  - **5. Spoofing**
    - Spoofing is the process of impersonating someone by tampering with the authentication process using a username and password.
    - Hackers can use spoofing to access personal information in a victim's account.
    - Spoofing mostly occurs in applications that use the Chakra scripting engine, such as Microsoft's Internet Explorer and Edge.

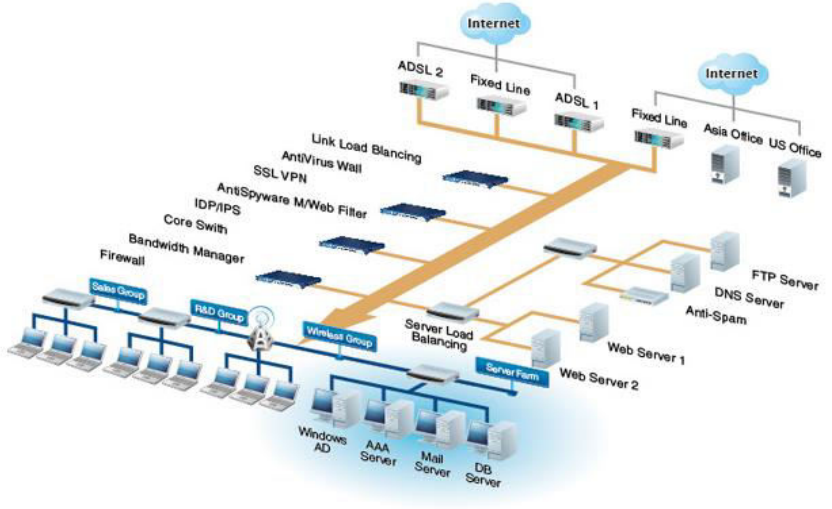
System Vulnerabilities

- The most common software security vulnerabilities include:
  - Missing data encryption
  - OS command injection
  - SQL injection
  - Buffer overflow
  - Missing authentication for critical function
  - Missing authorization
  - Unrestricted upload of dangerous file types
  - Reliance on untrusted inputs in a security decision
  - Cross-site scripting and forgery
  - Download of codes without integrity checks
  - Use of broken algorithms
  - URL redirection to untrusted sites
  - Path traversal
  - Bugs
  - Weak passwords
  - Software that is already infected with virus

Network Security Systems



Network Security Systems



Network Security Systems

- It is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.
- Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Network Security Systems

- How does network security work?
  - There are many layers to consider when addressing network security across an organization.
  - Attacks can happen at any layer in the network security layers model, so your network security hardware, software and policies must be designed to address each area.
  - Network security typically consists of three different controls: physical, technical and administrative.

Network Security Systems

- **Physical Network Security**
  - Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on.
  - Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

Network Security Systems

- **Technical Network Security**
  - Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network.
  - Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Network Security Systems

- **Administrative Network Security**
  - Administrative security controls consist of security policies and processes that control user behaviour, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

References

- https://www.kaspersky.co.in/resource-center/threats/malware-system-vulnerability
- https://inside.battelle.org/blog-details/hardware-vs.-software-vulnerabilities
- https://whatis.techtarget.com/definition/hardware-vulnerability
- https://www.perforce.com/blog/kw/common-software-vulnerabilities
- https://purplesec.us/network-vulnerability/
- https://www.redteamsecure.com/blog/the-most-common-types-of-network-vulnerabilities

Module-3

Introduction to Information Security Policies, Procedures, Standards and Guidelines

Module-3: Information Security Policies, Procedures, Standards and Guidelines

- Information Security Policies
- Key Elements of Security Policy
- Security Standards, Guidelines & Frameworks
- Security Standards Organizations
- Information Security Laws, Regulations and Guidelines

Information Security Policies

- Security policies are the foundation of Security infrastructure.
- Without them, you cannot protect your company from possible lawsuits, lost revenue and bad publicity, not to mention basic security attacks.
- A security policy is a document or set of documents that describes, at a high level, the security controls that will be implemented by the company.

Information Security Policy

- An information security policy is a set of rules enacted by an organization to ensure that all users of networks or the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority.
- An information security policy governs the protection of information, which is one of the many assets a corporation needs to protect.
- Thinking logically, one would say that a policy should be as broad as the creators want it to be: basically, everything from A to Z in terms of IT security.

Definitions

- Policies
  - High level statement that provide guidance to workers who must make present and future decision
- Standards
  - Requirement statements that provide specific technical specifications
- Guidelines
  - Optional but recommended Specifications

Information Security Policy, Standards and Procedures

- What are they?
  - Let us break down each of these governance documents are, and how to take care of them.
- Information Policies – The "What"
  - Policies are the high-level statements that communicate a company's objectives.
  - Typically the philosophy of solving security problems that may arise.
  - It gives information about what the organization's objectives are, and how they are designed to protect the company's assets.

Information Security Policy, Standards and Procedures

- Information Standards – The "How Often/Much"
  - Policies and Standards are similar but do differ in some very important ways.
  - Standards go more in-depth and elaborate on the Policies.
  - Who will be involved in implementing the Standards?
  - What are the specific responsibilities of the associated departments?
  - Who does the Standard pertain to?
  - Who owns the individual Standard?
  - Specific requirements are laid out here for a comprehensive look at how each control area fits into the overall information security program.
  - Standards are most compliance requirements and frameworks ask for.

Information Security Policy, Standards and Procedures

- Information Procedures – The "How"
  - Procedures are the step-by-step instructions for fulfilling the Policies and Standards.
  - For every control area your Policy covers, there needs to be corresponding sections for how the company will carry out that Policy.
  - Procedures take Policies and Standards creates tangible action steps.
  - In these procedures, the business should call out specific employees and technologies that are used to carry out each procedure.

What Information Security Policies are expected to do?

- Policies are not technology specific and do three things for an organization:
  i. Reduce or eliminate legal liability to employees and third parties.
  ii. Protect confidential, proprietary information from theft, misuse, unauthorized disclosure or modification.
  iii. Prevent waste of company computing resources.

Information Security Policy, Standards and Procedures

- The objectives of an IT security policy is the preservation of confidentiality, integrity, and availability of systems and information used by an organization's members.
- Three principles comprises the CIA triad:
  - **Confidentiality** involves the protection of assets from unauthorized entities
  - **Integrity** ensures the modification of assets handled in a specified and authorized manner
  - **Availability** is a state of the system in which authorized users have continuous access to said assets

Information Security Policy, Standards and Procedures

- The IT Security Policy is a living document that is continually updated to adapt with evolving business and IT requirements.
- Institutions such as the **International Organization of Standardization (ISO)** and the **U.S. National Institute of Standards and Technology (NIST**) have published standards and best practices for security policy formation.
- As stipulated by the **National Research Council** (NRC), the specifications of any company policy should address:
  1. Objectives
  2. Scope
  3. Specific goals
  4. Responsibilities for compliance and
  5. Actions to be taken in the event of noncompliance.

Why an organization/Company need them?

- Goal of an organizational information security policy is to provide relevant direction and value to the individuals within an organization with regard to security.
- A few core reasons why your organization should have information security policies:
  - Information security policies define what is required of an organization's employees from a security perspective
  - Information security policies reflect the risk appetite of an organization's management and should reflect the managerial mindset when it comes to security
  - Information security policies provide direction upon which a control framework can be built to secure the organization against external and internal threats
  - Information security policies are a mechanism to support an organization's legal and ethical responsibilities
  - Information security policies are a mechanism to hold individuals accountable for compliance with expected behaviors with regard to information security

Why an organization/Company need them?

- Establishes Continuity
  - Showing your employees exactly what is expected of them is crucial. Without a clear vision set, there will be inevitable questions. Creating a universal guide for everyone to see and understand will unify the team in times of crisis or confusion.
- Allows Easy Enforcement
  - Without implementing a governance program Executives will have no way to enforce the practices they want employees to follow. If these expectations are laid out clearly in easy to find Policies, Standards, and Procedures there will be proof to hold people accountable for not abiding by them.
- Creates a Security Culture
  - Usually if an Executive is involved in the creation of Policies, Standards, and Procedures they're more likely to understand what's happening when problems arise.
  - It makes easier for IT professionals, and other employees, to communicate and understand what is important to the Executives.

Why an organization/Company need them?

- Also mandatory for every IT security policy are **sections dedicated** to the adherence to regulations that govern the organization's industry.
  - For E.g. PCI Data Security Standard and the Basel Accords worldwide, or the Dodd-Frank Wall Street Reform, the Consumer Protection Act, the Health Insurance Portability and Accountability Act, and the Financial Industry Regulatory Authority in the United States.
- Many of these regulatory entities require a written IT security policy themselves.
- An organization's security policy will play a large role in its decisions and direction, but it **should not alter its strategy or mission.**
- It is important to write a **policy that is drawn from the organization's existing cultural and structural framework** to support the continuity of good productivity and innovation, and not as a generic policy that impedes the organization and its people from meeting its mission and goals.

What Should An Information Security Policy Include?

- Security policies should reflect the risk appetite of executive management in an organization.
- Write a policy that appropriately guides behavior to reduce the risk.
- If an organization has a risk regarding social engineering, then there should be a policy reflecting the behavior desired to reduce the risk of employees being socially engineered.
- Every employee must take yearly security awareness training (which includes social engineering tactics).
- Since information security itself covers a wide range of topics, a company information security policy (or policies) are commonly written for a broad range of topics such as the following:
  - Access control
  - Identification and Authentication (including multi-factor authentication and passwords)
  - Data classification
  - Encryption
  - Remote access
  - Acceptable use
  - Patching
  - Malicious code protections
  - Physical security
  - Backups
  - Server security (e.g. hardening)
  - Employee on/offboarding
  - Change management

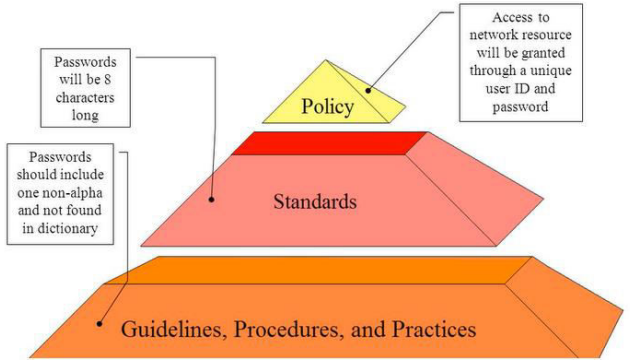
Challenges

- Define security policies and standards
- Measure actual security against policy
- Report violations to policy
- Correct violations to conform with policy
- Summarize policy compliance for the organization

How to Get Started!!!

1. Figure Out Your Needs
   - What an organization's size or niche is will mandate what their governance documents should be. If you have a large business with several employees, you may need a more detailed plan. If you have a small organization with people who do a little of everything, you should consider what guidelines to put in place to enable employees to effectively perform their job duties in a secure manner.
2. Build an Action Plan
   - Next, address how to get the governance program in place. Talk with your IT operations team to make sure they are in compliance with the program you are trying to build. If not, find out what resources and tools they need to achieve the organization's security goals.
3. Maintain and Update
   - Last, once you have your Policies, Standards, and Procedures in place, the work is not finished. Maintaining and updating your documents is just as important as the initial creation process. Times change, and so should your security governance. Be sure to do annual reviews of all these important documents to proactively evaluate the security controls related to the confidentiality, integrity, and availability of your business' sensitive information.

Security policy



- https://www.itgovernance.co.uk/blog/5-information-security-policies-your-organisation-must-have
- https://www.itgovernance.co.uk/shop/product/iso-27001-information-security-policy-template

Information Security Policies

- Types of basic security policies:
  1. **Technical security policies:** these include how technology should be configured and used.
  2. **Administrative security policies**: these include how people (both end users and management) should behave/ respond to security.

Information Security Policies

- Persons responsible for the implementation of the security policies are:
  - Director of Information Security
  - Chief Security Officer
  - Director of Information Technology
  - Chief Information Officer

Information Security Policies

- Guidelines for Effective Policy
  - Developed using industry-accepted practices
  - Distributed using all appropriate methods
  - Reviewed or read by all employees
  - Understood by all employees
  - Formally agreed to by act or assertion
  - Uniformly applied and enforced

Information Security Policies

- Developing Information Security Policy
  1. Investigation Phase
  2. Analysis Phase
  3. Design Phase
  4. Implementation Phase
  5. Maintenance Phase

Information Security Policies

1) Investigation Phase
  - Support from senior management
  - Support and active involvement of IT management
  - Clear articulation of goals
  - Participation by the affected communities of interest
  - Detailed outline of the scope of the policy development project

Information Security Policies

2) Analysis Phase
  - A new or recent risk assessment or IT audit documenting the information security needs of the organization.
  - Gathering of key reference materials – including any existing policies

Information Security Policies

3) Design Phase
- Users or organization members acknowledge they have received and read the policy
  - Signature and date on a form
  - Banner screen with a warning

Information Security Policies

4) Implementation Phase
- Policy development team writes policies
- Resources:
  - The Web
  - Government sites such as NIST
  - Professional literature
  - Peer networks
  - Professional consultants

Information Security Policies

5) Maintenance Phase
- Policy development team responsible for monitoring, maintaining, and modifying the policy

Information Security Policies

- Policy Distribution
  - Hand policy to employees
  - Post policy on a public bulletin board
  - E-mail
  - Intranet
  - Document management system

Information Security Policies

- A security policy should determine rules and regulations for the following systems:
  - Encryption mechanisms
  - Access control devices
  - Authentication systems
  - Firewalls
  - Anti-virus systems
  - Websites
  - Gateways
  - Routers and switches
  - Necessity of a security policy
- Policies for Application, Server, Network, etc.,.

Information Security Policies

Access Control Policy	How information is accessed
Contingency Planning Policy	How availability of data is made online 24/7
Data Classification Policy	How data are classified
Change Control Policy	How changes are made to directories or the file server
Wireless Policy	How wireless infrastructure devices need to be configured
Incident Response Policy	How incidents are reported and investigated
Termination of Access Policy	How employees are terminated
Backup Policy	How data are backed up
Virus Policy	How virus infections need to be dealt with

Information Security Policies

Retention Policy	How data can be stored
Physical Access Policy	How access to the physical area is obtained
Security Awareness Policy	How security awareness are carried out
Audit Trail Policy	How audit trails are analyzed
Firewall Policy	How firewalls are named, configured etc.
Network Security Policy	How network systems can be secured
Encryption Policy	How data are encrypted, the encryption method used etc.
Others	Promiscuous Policy Firewall Management Policy Permissive Policy

Information Security Policies

- Acceptable Encryption Policy
  - Outlines the requirement around which encryption algorithms (e.g. received substantial public review and have been proven to work effectively) are acceptable for use within the enterprise.
- Acceptable Use Policy
  - Defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.
- Acquisition Assessment Policy
  - Defines responsibilities regarding corporate acquisitions, and defines the minimum requirements of an acquisition assessment to be completed by the Infosec Team.
- Analog/ISDN Line Security Policy
  - Explains acceptable use of analog and ISDN lines and approval policies and procedures.
- Anti-Virus Guidelines
  - Defines guidelines for effectively reducing the threat of computer viruses on the organization's network
- Automatically Forwarded Email Policy
  - Documents the requirement that no email will be automatically forwarded to an external destination without prior approval from the appropriate manager or director.

Information Security Policies

- Bluetooth Baseline Requirements Policy
  - Defines the minimum baseline standard for connecting Bluetooth enabled devices to the enterprise network or company owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential company information.
- Clean Desk Policy
  - Defines the minimum requirements for maintaining a "clean desk" - where sensitive/critical information about our employees, our intellectual property, our customers, and our vendors is secure in locked areas and out of sight.
- Communications Equipment Policy
  - Defines the requirements for secure configurations of communication equipment.
- Data Breach Response Policy
  - Defines the goals and the vision for the breach response process. This policy defines to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms.
- Database Credentials Policy
  - Defines the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of company's networks.

Information Security Policies

- Dial In Access Policy
  - Defines the requirement for Dial-in/remote access to company computing resources.
- Digital Signature Acceptance Policy
  - Defines the requirements for when a digital signature is considered an accepted means of validating the identity of a signer in electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization.
- Disaster Recovery Plan Policy
  - Defines the requirement for a baseline disaster recovery plan to be developed and implemented by the company, which describes the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.
- DMZ Lab Security Policy
  - Documents the security requirements for all networks and equipment deployed in labs located on the "De-Militarized Zone" (DMZ) for the purpose of reducing or eliminating risks.
- Email Policy
  - Defines the requirements for proper use of the company email system and make users aware of what is considered acceptable and unacceptable use of its email system.
- Email Retention Policy
  - Defines the guidance to help employees determine what information sent or received by email should be retained and for how long.

Information Security Policies

- Employee Internet Use Monitoring and Filtering Policy
  - Defines the standards for systems that monitor and limit web use from any host within the company's network.
- End User Encryption Key Protection Plan
  - Defines the requirements for protecting encryption keys that are under the control of end users.
- Ethics Policy
  - Defines the guidelines and expectations of individuals within the company to demonstrate fair business practices and encourage a culture of openness and trust.
- Extranet Policy
  - Defines the requirement that third-party organizations requiring access to the organization's networks must sign a third-party connection agreement.
- Information Logging Standard
  - Defines the specific requirements for information systems to generate appropriate audit logs that will integrate with an enterprise's log management function.
- Internet DMZ Equipment Policy
  - Defines the standards to be met by all equipment owned and/or operated by the organization that is located outside the organization's Internet firewalls (the demilitarized zone or DMZ).

Information Security Policies

- Internet Usage Policy
  - Define standards for systems that monitor and limit web use from any host within the company network.
- Lab Anti Virus Policy
  - Defines the requirements which must be met by all computers connected to company lab networks to ensure effective virus detection and prevention.
- Lab Security Policy
  - Defines requirements for labs (both internal and DMZ) to ensure that confidential information and technologies are not compromised, and that production services and interests of the organization are protected from lab activities.
- Mobile Device Encryption Policy
  - Defines the requirements for encrypting data at rest on employee mobile endpoints.
- Mobile Employee Endpoint Responsibility Policy
  - Defines the requirements for employees to protect their laptop/mobile device that is used to conduct company business.
- Pandemic Response Planning Policy
  - Defines the requirements for planning, preparation and performing exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process.

Information Security Policies

- Password Construction Guidelines
  - Defines the guidelines and best practices for the creation of strong passwords.
- Password Protection Policy
  - Defines the standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.
- Personal Communication Devices and Voicemail Policy
  - Defines the requirements for management personal communication devices and voicemail accounts.
- Remote Access Mobile Computing Storage
  - Defines authorized methods for controlling mobile computing and storage devices that contain or access information resources.
- Remote Access Policy
  - Defines standards for connecting to the organization's network from any host or network external to the organization.

Information Security Policies

- Remote Access Tools Policy
  - Defines the requirements for what type of remote desktop software can be used and how it must be configured.
- Removable Media Policy
  - Defines the requirements for use of removable media.
- Risk Assessment Policy
  - Defines the requirement that the Infosec Team has the authority to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.
- Router and Switch Security Policy
  - Defines standards for minimal security configuration for routers and switches inside a production network, or used in a production capacity.
- Security Response Plan Policy
  - Defines the requirement for business units supported by the Infosec Team to develop and maintain a security response plan.
- Server Audit Policy
  - Defines baseline configuration standards for servers installed on the company network. Relevant content was added to the new Workstation Configuration Standard.

Information Security Policies

- Server Malware Protection Policy
  - Defines the requirements for which server systems are required to have anti-virus and/or anti-spyware applications.
- Server Security Policy
  - Defines standards for minimal security configuration for servers inside the organization's production network, or used in a production capacity.
- Social Engineering Awareness Policy
  - Defines guidelines to provide awareness around the threat of social engineering and defines procedures when dealing with social engineering threats. Relevant content was added to the Acceptable Use Policy.
- Software Installation Policy
  - Defines the requirements around installation of third-party software on company owned devices.
- Technology Equipment Disposal Policy
  - Defines the requirements for proper disposal of electronic equipment, including hard drives, USB drives, CD-ROMs, and other storage media which may contain various kinds of company data, some of which may be considered sensitive.

Information Security Policies

- Virtual Private Network Policy
  - Defines the requirements to follow when using Remote Access IPSec or L2TP Virtual Private Network (VPN) to connect to the corporate network. Relevant content was added to the general Network Access Policy.
- Web Application Security Policy
  - Defines the requirement for completing a web application security assessment and guidelines for completing the assessment.
- Wireless Communication Policy
  - Defines the requirement for wireless infrastructure devices to adhere to wireless communication policy in order to connect to the company network.
- Wireless Communication Standard
  - Defines the technical requirements that wireless infrastructure devices must satisfy in order to connect to the company network.
- Workstation Security (For HIPAA) Policy
  - Defines the requirements to ensure the HIPAA Security Rule "Workstation Security" Standard 164.310(c) can be met.

Managing Security Controls

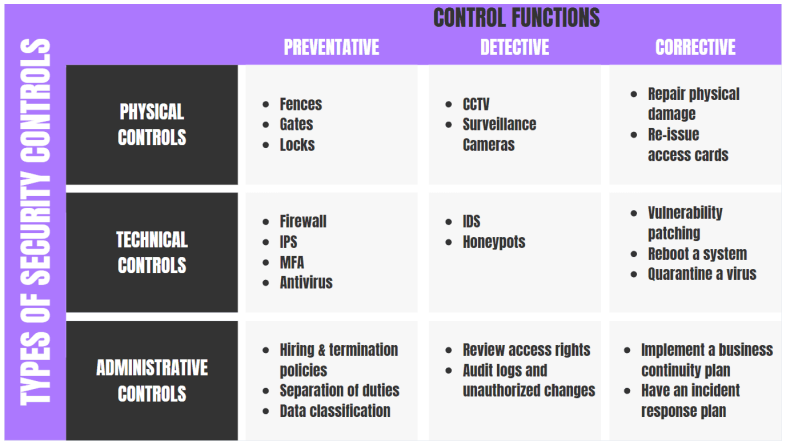
Security Controls

- Security controls play a foundational role in shaping the actions cyber security professionals take to protect an organization.
- There are three main types of IT security controls including technical, administrative, and physical.
- The primary goal for implementing a security control can be preventative, detective, corrective, compensatory, or act as a deterrent.
- Controls are also used to protect people as is the case with social engineering awareness training or policies.

What Is A Security Control?

- Security controls are countermeasures or safeguards used to reduce the chances that a threat will exploit a vulnerability.
- For example, implementing company-wide security awareness training to minimize the risk of a social engineering attack on your network, people, and information systems.
- The act of reducing risk is also called risk mitigation.

Security Controls



Risk Mitigation

- Risk mitigation is achieved by implementing different types of security controls depending on:
  - The goal of the countermeasure or safeguard.
  - The level to which the risk needs to be minimized.
  - The severity of damage the threat can inflict.

Risk Mitigation

What are the Goals of Security Controls?

- The overall purpose of implementing security controls as previously mentioned is to help reduce risks in an organization.
- In other words, the primary goal of implementing security controls is to prevent or reduce the impact of a security incident.
- The effective implementation of a security control is based on its classification in relation to the security incident.

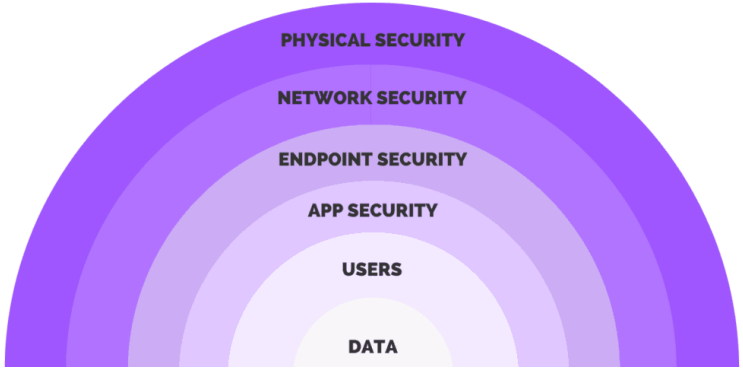
What are the Goals of Security Controls?

- The common classifications types are listed below along with their corresponding description:
  - Preventive controls attempt to prevent an incident from occurring.
  - Detective controls attempt to detect incidents after they have occurred.
  - Corrective controls attempt to reverse the impact of an incident.
  - Deterrent controls attempt to discourage individuals from causing an incident.
  - Compensating controls are alternative controls used when a primary control is not feasible.
- For example, an organization that places a high priority on reducing risk usually has a risk profile, which illustrates the potential cost of a negatively impacting risk and the human resources required to implement the control(s).

Layering Security Controls

- Layering is an approach that combines multiple security controls to develop what's called a defense-in-depth strategy.
- Defense-in-depth is a common strategy used in cyber security whereby multiple layers of controls are implemented.
- By combining controls into multiple layers of security you ensure that if one layer fails to counteract a threat that other layers will help to prevent a breach in your systems.
- Each layer of security works to counteract specific threats, which requires cyber security programs to invest in multiple technologies and processes to prevent systems or people from being compromised.
- For example, Endpoint detection and response solutions are great at preventing viruses and malware from infecting computers and servers.
- However, endpoint detection is not equipped to log and monitor traffic on a network like a SIEM, or detect and prevent an attack in real-time like an IPS.

Layering Security Controls



Understanding The Basics Of Risks & Threats

- Risks:
  - Risks in cyber security are the likelihood that a threat will exploit a vulnerability resulting in a loss. Losses could be information, financial, damage to reputation, and even harm customer trust.
- Threats:
  - Threats are any event with the potential to compromise the confidentiality, integrity, and availability (CIA) of information.
  - Threats come from outside an organization and from anywhere in the world connected to the internet. Insiders such as a disgruntled employee with too much access, or a malicious insider also pose a threat to businesses.
  - Note, insider threats are not always malicious. For example, an employee clicking on a phishing email that installs malware does not mean the employee intended to cause harm.
  - Finally, threats may also take the form of a natural disaster or be a manmade risk such as a new malware variant.

Understanding The Basics Of Risks & Threats

- Vulnerabilities
  - Vulnerabilities are a weakness or flaw in the software, hardware, or organizational processes, which when compromised by a threat, can result in a security incident.
- Security Incidents
  - Security incidents are an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Module-3

Security Standards,
Guidelines & Frameworks

Security Governance framework

- Adapted from ISO 38500.
- IT security governance is the system by which an organization directs and controls IT security.
- IT security governance should not be confused with IT security management.
- IT security management is concerned with making decisions to mitigate risks.
- IT governance determines the authorized personnel to make decisions.

Security Governance framework

- Security governance framework
  - Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks.
  - Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

Security Governance framework

- Five general governance areas
  - Govern the operations of the organization and protect its critical assets
  - Protect the organization's market share and stock price (perhaps not appropriate for education)
  - Govern the conduct of employees (educational AUP and other policies that may apply to use of technology resources, data handling, etc.)
  - Protect the reputation of the organization
  - Ensure compliance requirements are met

Security Governance framework

- 3 major frameworks
  1. COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  2. COBIT (Control Objectives for Information and Related Technology)
  3. ITIL (Information Technology Infrastructure Library)

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - In 1985, the Committee of Sponsoring Organizations of the Treadway Commission **(COSO)** developed a model for evaluating internal controls.
  - This model has been adopted as the generally accepted framework for internal control.
  - It is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Internal Control: Internal controls are the mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.
  - The updated COSO principles, which supersedes the original 1992 framework, now explicitly describes its principles rather than simply implying them, thus making it easier for companies to apply the principles.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - These concepts shows relationship between people and process the effective control define the principles and the way to implement them.
  - Internal control is the process and not a one-time activity.
  - Internal control affected by people; it must be adopted through the organization and is not simply a policy document that gets filled away.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Internal control can provide only reasonable assurance.
  - Internal control are designed for the achievement of business objectives.
  - A control cannot ensure success.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- 5 Components of COSO Internal control framework

5 Components of COSO

- *Control Environment*
  - Exercise integrity and ethical values.
  - Make a commitment to competence.
  - Use the board of directors and audit committee.
  - Facilitate management's philosophy and operating style.
  - Create organizational structure.
  - Issue assignment of authority and responsibility.
  - Utilize human resources policies and procedures.
- *Risk Assessment*
  - Create companywide objectives.
  - Incorporate process-level objectives.
  - Perform risk identification and analysis.
  - Manage change.

5 Components of COSO

- *Control Activities*
  - Follow policies and procedures.
  - Improve security (application and network).
  - Conduct application change management.
  - Plan business continuity/backups.
  - Perform outsourcing.
- *Information and Communication*
  - Measure quality of information.
  - Measure effectiveness of communication.
- *Monitoring*
  - Perform ongoing monitoring.
  - Conduct separate evaluations.
  - Report deficiencies.

Control Objectives for Information and Related Technology (COBIT)

- COBIT stands for Control Objectives for Information and Related Technology
- A framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management
- Supports managers allows balancing technical issues, business risks and control requirements
- Ensures quality, control and reliability of information systems in organization

Control Objectives for Information and Related Technology (COBIT)

- Used by all organizations whose primary responsibilities happen to be business processes and related technologies
- Helps in increasing the sensibility of IT processes to a great extent
- Helps organizing the objectives of IT governance and bringing in the best practices in IT processes and domains, while linking business requirements
- Used by both the government departments, federal departments and other private commercial organizations

Control Objectives for Information and Related Technology (COBIT)

- COBIT – 7 control areas:
  - Effectiveness: Information should be delivered in timely, correct, consistent and usable manner.
  - Efficiency: Information delivered cost effective
  - Confidentiality: Data protection from unauthorized disclosure.
  - Integrity: Protection of manipulation of data
  - Availability: Data accessible 24 X 7
  - Compliance: Adherence to laws, regulation and contractual agreements.
  - Reliability of Information: Data correctly represents the state of business.

Control Objectives for Information and Related Technology (COBIT)

- IT resources in COBIT are the components of information delivery and represent the technology, people and procedures used to meet business goals.
- Resources are divided into four areas:
  1. Application
  2. Information
  3. Infrastructure
  4. People

Control Objectives for Information and Related Technology (COBIT)

- Domain and process of COBIT
  1. Plan and Organize (PO)
  2. Acquire and Implement (AI)
  3. Deliver and Support (DS)
  4. Monitor and Evaluate (ME)

Control Objectives for Information and Related Technology (COBIT)

- Domain and process of COBIT
  1. Plan and Organize
     - The Planning and Organization domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives.

PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects

Control Objectives for Information and Related Technology (COBIT)

- Domain and process of COBIT
  2. Acquire and Implement (AI)
     - It covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes.

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and Changes

Control Objectives for Information and Related Technology (COBIT)

- Domain and process of COBIT
  3. Deliver and Support (DS)
     - It focuses on the delivery aspects of the information technology.

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Control Objectives for Information and Related Technology (COBIT)

- Domain and process of COBIT
  4. Monitor and Evaluate (ME)
     - The Monitoring and Evaluation domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements.

Control Objectives for Information and Related Technology (COBIT)

- Domain and process of COBIT
  4. Monitor and Evaluate (ME)

ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Compliance with External Requirements
ME4	Provide IT Governance

Control Objectives for Information and Related Technology (COBIT)

- The COBIT Maturity Model scale provides the following measurements:
  - 0 Non existent
  - 1 Initial/ Ad hoc
  - 2 Repeatable
  - 3 Defined process
  - 4 Managed
  - 5 Optimized

Control Objectives for Information and Related Technology (COBIT)

COBIT Maturity Scale

0 Non existent
Not performed.

1 Initial/ Ad hoc
Process is chaotic, not standardized and done case by case.

2 Repeatable
Relies on individual knowledge, no formal training and no process intuitive management.

3 Defined process
Standardized and documented processes and formal training to communicate standards.

4 Managed
Processes are monitored and checked for compliance by management, measurable processes are reviewed for improvement and limited automation.

5 Optimized
Processes are refined and compared with others based on maturity, processes are automated through workflow tools to improve quality and effectiveness.

ITIL security management (Information Technology Infrastructure Library)

- ITIL security management is based on the ISO 27001 standard.
- "ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, non-for profit organizations).
- The Primary **objective of ITIL Information Security Management Process** (ITIL ISM) is to align IT security with business security and ensure that information security is effectively managed in all service and IT Service Management activities.
- It also ensures the confidentiality, integrity, availability, and role-based accessibility of an organization's assets, information, data and IT Services are maintained.

ITIL security management (Information Technology Infrastructure Library)

- 5 Stages of the ITIL-V3
  1. **Service Strategy:**
     - The Service Strategy phase of the Service Lifecycle provides guidance on how to design, develop, and implement IT Service Management.
  2. **Service Design:**
     - The Service Design phase of the Service Lifecycle provides guidance on how to design and develop services and IT Service Management processes that will support the service strategies already developed.
  3. **Service Transition:**
     - The Service Transition phase of the Service Lifecycle teaches IT professionals and their business associates to manage changes in a productive manner.

ITIL security management (Information Technology Infrastructure Library)

- 5 Stages of the ITIL-V3
  4. **Service Operation:**
     - The Service Operation phase of the Service Lifecycle provides guidance on the practical aspects of day-to-day business operations.
     - The goal is for the IT department to keep things running smoothly, reliably, efficiently and cost-effectively.
  5. **Continual Service Improvement:**
     - Even if nothing changes in an organization, there is always room for development and improvement in IT services.
     - Continual assessment is the key to understanding where improvements can be made.

Module 3

Information Security Management

Monitor systems and apply controls - security assessment using automated tools

Security Assessment
Outline

- What is security assessment?
- What are the non-intrusive types?
- How do you choose between these types?
- What are the intrusive types?
- What are the types of risk reduction?
- What is effective security?
- What are the limitations to security assessment?

Security Assessment
Overview

- Definition
  - Security assessment
    - identifies existing IT vulnerabilities (weakness) and
    - recommends countermeasures for mitigating potential risks
- Goal
  - Make the infrastructure more secure
  - Identify risks and reduce them
- Consequences of Failure
  - Loss of services
  - Financial loss
  - Loss of reputation
  - Legal consequences

Security Assessment
Types

- Non-Intrusive
  1. Security Audit
  2. Risk Assessment
  3. Risk Analysis
- Intrusive
  1. Vulnerability Scan
  2. Penetration Testing / Ethical Hacking
- All have the goal of identifying vulnerabilities and improving security
  - Differ in rules of engagement and limited purpose of the specific engagement (what is allowed, legal liability, purpose of analysis, etc.).

Security Assessment: Non-Intrusive Types
1. Security Audit

- **Security Audit**- Independent review and examination of system records & activities to determine adequacy of system controls, ensure compliance of security policy & operational procedures, detect breaches in security, and recommend changes in these processes.[1]
- Features
  - Formal Process
  - Paper Oriented
    - Review Policies for Compliance and Best Practices
  - Review System Configurations
    - Questionnaire, or console based
  - Automated Scanning
  - Checklists

1 http://www.atis.org/tg2k/_security_audit.html

Security Assessment: Non-Intrusive Types

2. Risk Assessment

- **Risk Assessment** (Vulnerability Assessment) is:
  - determination of state of *risk* associated with a system based upon thorough *analysis*
  - includes recommendations to support subsequent security *controls*/decisions.
  - takes into account business, as well as legal *constraints*.
- Involves more testing than traditional paper audit
- Primarily required to identify weaknesses in the information system
- Steps
  - Identify security holes in the infrastructure
  - Look but not intrude into the systems
  - Focus on best practices (company policy is secondary)

Security Assessment: Non-Intrusive Types

3. Risk Analysis

- **Risk Analysis** is the identification or study of:
  - an organization's *assets*
  - *threats* to these *assets*
  - system's *vulnerability* to the *threats*
- Risk Analysis is done in order to determine *exposure* and potential *loss*.
- Computationally intensive and requires data to
  - Compute probabilities of attack
  - Valuation of *assets*
  - Efficacy of the *controls*
- More cumbersome than *audit* or *assessment* and usually requires an analytically trained person

Security Assessment

How to choose

- Security audit, risk assessment and risk analysis have similar goals.

Security Assessment

Assessment vs. Analysis vs. Audit

	Assessment	Analysis	Audit
Objective	Baseline	Determine Exposure and Potential Loss	Measure against a Standard
Method	Various (including use of tools)	Various (including tools)	Audit Program/ Checklist
Deliverables	Gaps and Recommendations	Identification of Assets, Threats & Vulnerabilities	Audit Report
Performed by:	Internal or External	Internal or External	Auditors
Value	Focused Improvement	Preparation for Assessment	Compliance

Security Assessment: Intrusive Types
1. Vulnerability Scan

- Definition
  - Scan the network using automated tools to identify security holes in the network
- Usually a highly automated process
  - Fast and cheap
- Limitations
  - False findings
  - System disruptions (due to improperly run tools)
- Differences in regular scans can often identify new vulnerabilities

Security Assessment: Intrusive Types
2. Penetration Testing

- Definition (Ethical Hacking)
  - Simulated attacks on computer networks to identify weaknesses in the network.
- Steps
  - Find a vulnerability
  - Exploit the vulnerability to get deeper access
  - Explore the potential damage that the hacker can cause
- Example
  - Scan web server: Exploit buffer overflow to get an account
  - Scan database (from web server)
  - Find weakness in database: Retrieve password
  - Use password to compromise firewall

Security Assessment
Risk Reduction

There are three strategies for risk reduction:

- Avoiding the risk
  - by changing requirements for security or other system characteristics
- Transferring the risk
  - by allocating the risk to other systems, people, organizations assets or by buying insurance
- Assuming the risk
  - by accepting it, controlling it with available resources

Security Assessment
Effective Security

- Effective security relies on several factors
  - Security Assessments
  - Policies & Procedures
  - Education (of IT staff, users, & managers)
  - Configuration Standards/Guidelines
    - OS Hardening
    - Network Design
    - Firewall Configuration
    - Router Configuration
    - Web Server Configuration
  - Security Coding Practices

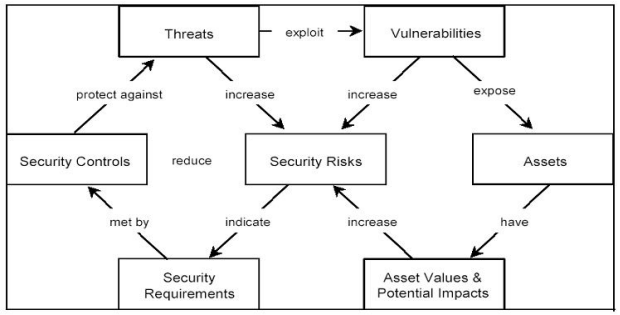
Security Assessment
Limitations

- Often locates previously known issues
  - Provides false sense of security
- Just the first step
  - Needs due diligence in applying the recommendation of the assessment
- Becomes obsolete rapidly
  - Needs to be repeated periodically

What is Security Assessment?
Case

- **Scenario to identify the suitable method for application to the scenario**

Risk Analysis
Concept Map



• Threats exploit system vulnerabilities which expose system assets.

• Security controls protect against threats by meeting security requirements established on the basis of asset values.

Risk Analysis
Basic Definitions

- **Assets**- Something that the agency values and has to protect. Assets include all information and supporting items that an agency requires to conduct business.
- **Vulnerability**- A weak characteristic of an information *asset* or group of assets which can be exploited by a *threat*.[1] Consequence of weaknesses in *controls*.
- **Threat**- Potential cause of an unwanted event that may result in harm to the agency and its *assets*.[1] A threat is a manifestation of *vulnerability*.
- **Security Risk**- is the probability that a specific *threat* will successfully exploit a *vulnerability* causing a *loss*.
- **Security Controls**- Implementations to reduce overall *risk* and *vulnerability*.

1 http://www.oit.nsw.gov/au/pdf/4.4.16.IS1.pdf

Risk Analysis
Assets

- Assets: Something that the agency values and has to protect. Assets include all information and supporting items that an agency requires to conduct business.
- Data
  - Breach of confidentiality
  - Loss of data integrity
  - Denial of service
  - Corruption of Applications
  - Disclosure of Data
- Organization
  - Loss of trust
  - Embarrassment
  - Management failure
- Personnel
  - Injury and death
  - Sickness
  - Loss of morale

Risk Analysis
Assets Cont'd

- Infrastructure
  - Electrical grid failure
  - Loss of power
  - Chemical leaks
  - Facilities & equipment
  - Communications
- Legal
  - Use or acceptance of unlicensed software
  - Disclosure of Client Secrets
- Operational
  - Interruption of services
  - Loss/Delay in Orders
  - Delay in Shipments

Risk Analysis
Vulnerabilities

- Vulnerabilities are flaws within an asset, such as an operating system, router, network, or application, which allows the asset to be exploited by a threat.
- Examples
  - Software design flaws
  - Software implementation errors
  - System misconfiguration (e.g. misconfigured firewalls)
  - Inadequate security policies
  - Poor system management
  - Lack of physical protections
  - Lack of employee training (e.g. passwords on post-it notes in drawers or under keyboards)

Risk Analysis
Threats

- Threats are potential causes of events which have a negative impact.
  - Threats exploit vulnerabilities causing impact to assets
- Examples
  - Denial of Service (DOS) Attacks
  - Spoofing and Masquerading
  - Malicious Code
  - Human Error
  - Insider Attacks
  - Intrusion

Risk Analysis
Sources of Threats

Source	Examples of Reasons
External Hackers with Malicious Intent	• Espionage • Intent to cause damage • Terrorism
External Hackers Seeking Thrill	• Popularity
Insiders with Malicious Intent	• Anger at company • Competition with co-worker(s)
Accidental Deletion of Files and Data	• User errors
Environmental Damage	• Floods • Earthquakes • Fires
Equipment and Hardware Failure	• Hard disk crashes

Risk Analysis
Security Risk

- Risk is the probability that a specific *threat* will successfully exploit a *vulnerability* causing a *loss*.
- Risks of an organization are evaluated by three distinguishing characteristics:
  - loss associated with an event, e.g., disclosure of confidential data, lost time, and lost revenues.
  - likelihood that event will occur, i.e. probability of event occurrence
  - Degree that risk outcome can be influenced, i.e. controls that will influence the event
- Various forms of threats exist
- Different stakeholders have various perception of risk
- Several sources of threats exist simultaneously

Risk Analysis
Physical Asset Risks

- Physical Asset Risks
  - Relating to items with physical and tangible items that have an associated financial value

Risk Analysis
Mission Risks

- Mission Risks
  - Relating to functions, jobs or tasks that need to be performed

Risk Analysis
Security Risks

- Security Risks
  - Integrates with both asset and mission risks

Risk Analysis: Definitions and Nomenclature
Question 1

1) From the concept map, fill in the blanks:

Vulnerabilities are exploited by_____.

_____ are used to diminish risk from threats.

To determine _____ it is necessary to know the values of assets as well as the _____ to threats.

Knowledge of security _____ is necessary before deciding on controls to implement.

Risk Analysis: Definitions and Nomenclature
Question 2

2) Match the type of asset to the potential threat

Organization	Stolen Credit Card Numbers
Operational	Air Traffic Radar Failure
Data	Loss of Orders
Legal	System Administrator's Death
Personnel	Loss of Reputation
Infrastructure	Denial of Service

Risk Analysis: Definitions and Nomenclature
Question 3

3) Threat or Vulnerability ? Place a T next to an example of a threat and a V next to an example of a vulnerability

_____ Misconfigured firewall
_____ Denial of Service
_____ Unpatched operating system
_____ Theft
_____ Hard Drive Failure
_____ Unauthorized access to data
_____ Code within IE which allows for an attacker to execute malicious program
_____ Unlocked door
_____ Code Red Worm
_____ Weak passwords

Risk Analysis: Define Objectives

Standards

- ISO 17799
  - Title: Information technology -- Code of practice for information security management
  - Starting point for developing policies
  - http://www.iso.ch/iso/en/prods-services/popstds/.../en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35
- ISO 13335
  - Title: Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security
  - Assists with developing baseline security.
  - http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21733&ICS1=35
- NIST SP 800-xx
  - Different standards for various applications
  - http://csrc.nist.gov/publications/nistpubs/
- Center for Internet Security
  - Configuration Standards (benchmarks)
  - http://www.cisecurity.org/

Risk Analysis: Tools and Usage

Types

- Tools can speed up the security assessment and help in automation of the risk analysis process.
- Several categories of tools exist:
  - Asset Inventory
  - Software Usage
  - Vulnerability Assessment
  - Configuration Validation
  - Penetration Testing
  - Password Auditing
  - Documentation

Source: http://techrepublic.com.com/5100-6262-5060605-2.html

Risk Analysis: Tools and Usage

Asset inventory

Source: http://techrepublic.com.com/5100-6262-5060605-2.html

- Inventory process includes physical inventory and automated tools
- Physical inventory of IT assets that are not attached to the network
  - e.g. in storage closets or locally attached and that are thus not discoverable.
- Autodiscovery tools collect physical data on an enterprise's IT assets and record history of changes made to the asset from the last scan
  - e.g. memory, processor, and software version
- Inventory tools can either:
  - install an agent on the hardware device, which lets the inventory run even if the device is not attached to the network,
  - or be agentless, which can send information only when it is attached to the network.
- In environments with mobile set of assets that are sporadically connected (e.g. once a month), agentless technology requires alternatives way to capture the inventory
  - e.g. such as an e-mail that kicks off the scan.
- The assets that need to be discovered include
  - PDAs, PCs, networking equipment, and servers.

Risk Analysis: Tools and Usage

Asset Inventory Tools

Name	Description
Asset Tracker for Networks	Inventory software tool intended to audit software and hardware components installed on computers over a network. It collects network inventory information, provides detailed comprehensive reports and allows export of assets details to external storages, such as SQL database or web site. http://www.alchemy-lab.com/products/atn/
Asset Center	Peregrine Autodiscovery/inventory tool which maintains "an evolving snapshot of IT infrastructure" and provides: what hardware and software is available, asset connection to other assets, location of assets, access to assets, as well as financial and contractual information on assets. http://www.peregrine.com/products/assetcenter.asp
Unicenter Access Management	Computer Associates International asset management tool. It features: "automated discovery, hardware inventory, network inventory, software inventory, configuration management, software usage monitoring, license management and extensive cross-platform reporting." http://www3.ca.com/Solutions/Product.asp?ID=194

Tools

Asset Inventory Tools, cont'd.

Name	Description
Tally Systems	Tally Systems offers three tools which can be used for IT asset inventory. These are: TS Census Asset Inventory, WebCensus and PowerCensus. These products provide unparalleled IT asset inventory and tracking, hosted PC inventory and reporting, and enhanced inventory for Microsoft SMS respectively. http://www.tallysystems.com/products/itassettracking.html
Isogon	Isogon offers multiple tools. SoftAudit gathers software inventory and usage data from your z/OS, OS/390, or UNIX server. Asset insight offers PC, PDA, & network device auto-discovery software & captures data. Vista manages and organizes details from contracts, contract addenda/attachments, and maintenance agreements. http://www.isogon.com/SAM%20Solutions.htm

Risk Analysis: Tools and Usage

Software Usage

- Software usage tools monitor the use of software applications in an organization
- Several uses of such tools
  - Track usage patterns and report on trends to assist with server load balancing and license negotiation to prevent costly overbuying or risk-laden under buying.
  - Used to monitor and control the use of unauthorized applications (for example, video games and screen savers).
  - Important for vendor auditing the customers especially for monitoring clients for subscription-based pricing

Risk Analysis: Tools and Usage

Software Usage Tools

Name	Description
Software Audit Tool (GASP)	Designed to help detect and identify pirated software through tracking licenses. It is a suite of tools used by the Business Software Alliance and is freely available at: http://global.bsa.org/uk/antipiracy/tools/gasp.phtml

Risk Analysis: Tools and Usage

Vulnerability Assessment

- Vulnerability Assessment helps determine vulnerabilities in computer networks at any specific moment in time.
- Deliverables:
  - List of exploits and threats to which systems and networks are vulnerable. (Ranked according to risk levels)
  - Specific information about exploits and threats listed. (name of exploit or threat, how the threat/exploit works)
  - Recommendations for mitigating risk from these threats and exploits.
- Tools used can be:
  - Commercial or open source (decide based on staff skills)
  - Perform analysis such as:
  - Host-based or network-based

Risk Analysis: Tools and Usage

Vulnerability Assessment (Host or Network Based)

Host-based Tools	Network-Based Tools
Pros	Pros
Can provide rich security information, such as by checking user access logs.	Once deployed, have limited impact on network traffic.
Can give a quick look at what weaknesses hackers and worms can exploit.	Available as software, appliances and managed services.
Cons	Cons
Costs can add up when deploying agents across many desktops and servers.	Deployment can be time-consuming.
Requires careful planning to avoid conflict with security systems.	Generates considerable network traffic.

Source: http://www.nwfusion.com/news/2004/0405specialfocus.html

Risk Analysis: Tools and Usage

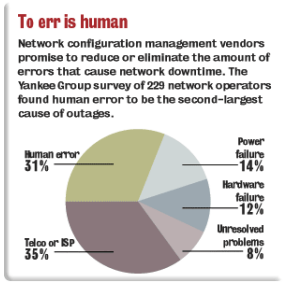
Vulnerability Assessment

Name	Description
Cerberus Internet Scanner	Windows web server vulnerability tester designed to help administrators locate and fix security holes in their computer systems http://www.cerberus-infosec.co.uk/cis.shtml
Cgichk	This is a web vulnerability scanner which searches interesting directories and files on a site. Looks for interesting and hidden directories such as logs, scripts, restricted code, etc. http://sourceforge.net/projects/cgichk/
Nessus	Server and client software vulnerability assessment tool which provides remote and local security checking. http://www.nessus.org/download.html
SAINT	SAINT (Security Administrator's Integrated Network Tool) is a security assessment tool. It scans through a firewall updated security checks from CERT & CIAC bulletins. Also, it features 4 levels of severity (red, yellow, brown, & green) through an HTML interface. Based on SATAN model. http://www.saintcorporation.com/products/saint_engine.html
SARA	SARA (Security Auditor's Research Assistant) Third generation UNIX-based security analysis tool. It contains: SANS/ISTS Certified, CVE standards support, an enterprise search module, standalone or daemon mode, user extension support and is based on the SATAN model http://www.www-arc.com/sara/
Nikto	A web server scanner which performs comprehensive tests against web servers for multiple items, including over 2200 potentially dangerous files/CGIs, versions on over 140 servers, and problems on over 210 servers http://www.cirt.net/code/nikto.shtml

Risk Analysis: Tools and Usage

Configuration Validation

- Configuration Validation
  - is the process in which the current configuration of a specific system, software, or hardware tool is tested against configuration guidelines.



- Human error is shown to be the 2nd largest reason for network downtime.
- Using configuration validation tools will help correct for human error

Source: http://nww1.com/news/2004/0216specialfocus.html

Risk Analysis: Tools and Usage

Configuration Validation

- Depending on focus, especially with network and OS configurations, configuration validation can utilize the same tools as vulnerability assessment & penetration testing
- However, there are more specialized tools for validating specific software applications and hardware.

Risk Analysis: Tools and Usage

Configuration Validation

Name	Description
Microsoft Baseline Security Analyzer	Method of identifying common security misconfigurations among Microsoft Windows NT 4.0, 2000, XP, 2003, IIS, SQL Server, Exchange Server, Media Player, Data Access Components (MDAC), Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, Host Integration Server & Office. http://www.microsoft.com/technet/security/tools/mbsahome.mspx
CISCO Router and Security Device Manager	This offers advanced configuration support for LAN and WAN interfaces, NAT, Stateful Firewall Policy, Inline Intrusion Prevention and IPSec virtual private network (VPN) features. It also provides a 1-click router lockdown and ability to check and recommend changes to router configuration based on ICSA Labs, and Cisco TAC recommendations." http://www.cisco.com/en/US/products/sw/secursw/ps5318/
Linux Configuration and Diagnostic Tools	This site provides a listing of various Linux configuration tools for system and network configuration, X configuration, library and kernel dependency management, and general diagnostics. http://www.comptechdoc.org/os/linux/usersguide/linux_ugdiag.html

Risk Analysis: Tools and Usage

Penetration Testing

- Penetration Testing is the evaluation of a system for weaknesses through attempting to exploit vulnerabilities.
- Can be done in-house or by a neutral 3rd party
- "Black-box" (no knowledge) or "White-box" (complete knowledge)
- Steps
  - Define scope (*External*: servers, infrastructure, underlying software; *Internal*: network access points; *Application*: proprietary applications and/or systems; *Wireless/Remote Access*; *Telephone/Voice Technologies*; *Social Engineering*)
  - Find correct tools (freeware or commercial software)
  - Properly configure tools to specific system
  - Gather information/data to narrow focus ("white-box")
  - Scan using proper tools
- Penetration Testing tools can include:
  - Network exploration (ping, port scanning, OS fingerprinting)
  - Password cracking
  - IDS, Firewall, Router, Trusted System, DOS, Containment Measures Testing
  - Application Testing and Code Review

Source: http://www.penetration-testing.com

Risk Analysis: Tools and Usage

Penetration Testing

Name	Description
Whois	Domain name lookup to find administrative, technical, and billing contacts. It also provides name servers for the domain. http://www.allwhois.com
Nmap	Utility for network exploration or security auditing. Can scan large networks or single hosts. It uses raw IP packets to determine hosts available on network, services those hosts are running, OS and OS version they are running, type of packet filters/firewalls being used, etc. http://www.insecure.org/nmap/nmap_download.html
MingSweeper	Network Reconnaissance Tool. Supports various TCP port & filter scans, UDP scans, OS detection (NMAP and ICMP style), Banner grabbing etc. http://www.hoobie.net/mingsweeper/
Cheops	Network mapping tool with graphical user interface (GUI). http://www.marko.net/cheops/
QueSO	Remote OS detector. Sends obscure TCP packets to determine remote OS. http://www.antiserver.it/Unix/scanner/Unix-Scanner/

Risk Analysis: Tools and Usage

Password Auditing

- Used for testing passwords for weaknesses which lead to vulnerable systems
- Reasons for password weakness
  - Poor encryption
  - Social engineering (e.g. password is spouse's, pet's or child's name)
  - Passwords less than 6 characters
  - Passwords do not contain special characters and numbers in addition to lower and uppercase letters.
  - Passwords from any dictionary
- Software tools might perform these tasks:
  - Extracting hashed passwords / encrypted passwords
  - Dictionary attack (cracks passwords by trying entries in a pre-installed dictionary)
  - Brute force attack (cracks passwords by trying all possible combinations of characters)
- Deliverables
  - Recommendations for future password policies

Risk Analysis: Tools and Usage

Password Auditing

Name	Description	OS
John the Ripper	Detects weak UNIX passwords. "Uses highly optimized modules to decrypt different ciphertext formats and architectures" Can be modified to crack LM hashes in Windows. http://www.openwall.com/john/	All platforms
Brutus	Remote password cracker. http://www.hoobie.net/brutus/	Windows
Magic Key	Audits the AppleTalk users file for weak passwords using brute force methods. http://freaky.staticusers.net/security/auditing/MK3.2.3a.sit	Macintosh
L0phtcrack	Assesses, recovers, and remediates Windows and Unix account passwords from multiple domains and systems. http://www.atstake.com/products/lc/	Windows & UNIX
SAMInside	Extracts information about users from SAM-files and performs brute force attack of Windows NT/2000/XP. Breaks defense of Syskey. http://www.topshareware.com/SAMInside-download-5188.htm	Windows
GetPass!	Cracks weakly encrypted Cisco IOS type 7 passwords once encrypted password file is obtained. http://www.networkingfiles.com/Network/downloads/bosongetpassdownload.htm	Cisco Router IOS
wwwhack	Brute force utility that will try to crack web authentication. Can use a word file or try all possible combinations, and by trial-and-error, will attempt to find a correct username/password combination. http://www.securityfocus.com/tools/1785	Windows

Risk Analysis: Tools and Usage

Documentation

- Documentation contains data from the risk analysis
- These documents should contain deliverables from other parts of the process (asset inventory, vulnerability assessment, etc.).
  - These can be provided automatically from specialized software or through compiled reports.
- Documentation critical for legal cases where it can be used as evidence to justify expense on controls.
- Documentation might include:
  - Focus of analysis
  - Current system vulnerabilities
  - Cost benefit analysis
  - Recommended controls

Module-3

Information Security Laws, Regulations & Guidelines

Information Security Laws, Regulations & Guidelines

- Information Security Law is the body of legal rules, codes, and standards that require you to protect that information and the information systems that process it, from unauthorized access.
- The legal risks are potentially significant if you don't take a pragmatic approach.
- Indian ministry of Communication and Information Technology has implemented IT-rules, 2011(Privacy rules).

Information Security Laws, Regulations & Guidelines

- India enabling legislation India Information Act 2000.
- While India continues to adhere to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules) enacted in 2011, the Centre for Internet and Society presented a new Privacy (Protection) Bill, 2013 (Bill), on September 30, 2013.

Information Security Laws, Regulations & Guidelines

- The Bill seeks to further refine provisions of the Rules, with a focus on protection of personal data through limitations on use and requirements for notice.
- The collection of personal data would be prohibited unless "necessary for the achievement of a purpose of the person seeking its collection," and, subject to sections 6 and 7 of the Bill, "no personal data may be collected under this Act prior to the data subject being given notice, in such form and manner as may be prescribed, of the collection."

Information Security Laws, Regulations & Guidelines

- **Data protection authority and registration requirement**
  - No specific data protection authority exists the privacy rule states that, in case of breach as defined under Act, must answer to" the agency mandated under the Law"
  - There re no registration required to collection of data.
  - Data security Council of India (DSCI) has providing "DSCI Privacy Certified" for data collection.

Information Security Laws, Regulations & Guidelines

- **Protected personal data**
  - Personal data is information that relates to an identified or identifiable individual.
  - What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

Information Security Laws, Regulations & Guidelines

- **Protected personal data**
  - If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
  - If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

Information Security Laws, Regulations & Guidelines

- **Data Collection and Processing**
  - The Privacy Rules requires a Body Corporate that collects, receives, possesses, stores, deals, or handles sensitive or personal data to provide a privacy policy for handling of such data and ensure that the policies are available for view by the data subjects who have provided the information under contract.

Information Security Laws, Regulations & Guidelines

- **Data Collection and Processing**
  - The policy shall provide for:
    - clear and easily accessible statements of its practices and policies;
    - the type of personal or sensitive personal data or information collected;
    - the purpose of collection and usage of such information;
    - the disclosure of information including sensitive personal data or information; and
    - reasonable security practices and procedures.

Information Security Laws, Regulations & Guidelines

- **Data Transfer**
  - Disclosure of data to a third party requires prior permission of the data subject, whether the information is provided under contract or otherwise, except in the following situations:
    - the disclosure has already been agreed to in a contract;
    - the disclosure is necessary for compliance with a legal obligation;
    - the data is shared with government agencies with the authority to obtain the data for the purpose of verification of identity, or for the prevention, detection, investigation, prosecution, and punishment of offenses, including cyber incidents; or
    - the disclosure is pursuant to an order under the law.

Information Security Laws, Regulations & Guidelines

- **Data Security**
  - A Body Corporate is required to implement reasonable security practices and procedures. The Privacy Rules indicate that reasonable practice methodologies include IS/ISO/EIC 27001 or other measures that have been pre-approved by the central government and are subject to annual audits by a central government approved auditor.

Information Security Laws, Regulations & Guidelines

- **Breach Notification**
  - There is no mandatory requirement to report data security breach incidents under the Privacy Rules

Information Security Laws, Regulations & Guidelines

- **Other Considerations**
  - Data retention rules state that information should not be retained longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law.
  - Accordingly, outsourcing service providers in India should be exempt from obtaining consent from the individuals whose data they process.

Information Security Laws, Regulations & Guidelines

- **Enforcement & Penalties**
  - A corporate entity may be liable for up to Rs. 50,000,000 for the negligent failure to implement and maintain reasonable practices and procedures, causing wrongful loss or gain.

Information Security Laws, Regulations & Guidelines

Broad laws:

- Sarbanes-Oxley Act (SOX);
- Payment Card Industry Data Security Standard (PCI DSS);
- Gramm-Leach-Bliley Act (GLB) Act;
- Electronic Fund Transfer Act, Regulation E (EFTA);
- Customs-Trade Partnership Against Terrorism (C-TPAT);
- Free and Secure Trade Program (FAST);
- Children's Online Privacy Protection Act (COPPA);
- Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule; Federal Rules of Civil Procedure (FRCP)

Information Security Laws, Regulations & Guidelines

Industry specific laws:

- Federal Information Security Management Act (FISMA);
- North American Electric Reliability Corp. (NERC) standards;
- Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records;
- Health Insurance Portability and Accountability Act (HIPAA);
- The Health Information Technology for Economic and Clinical Health Act (HITECH);
- Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule);
- H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation