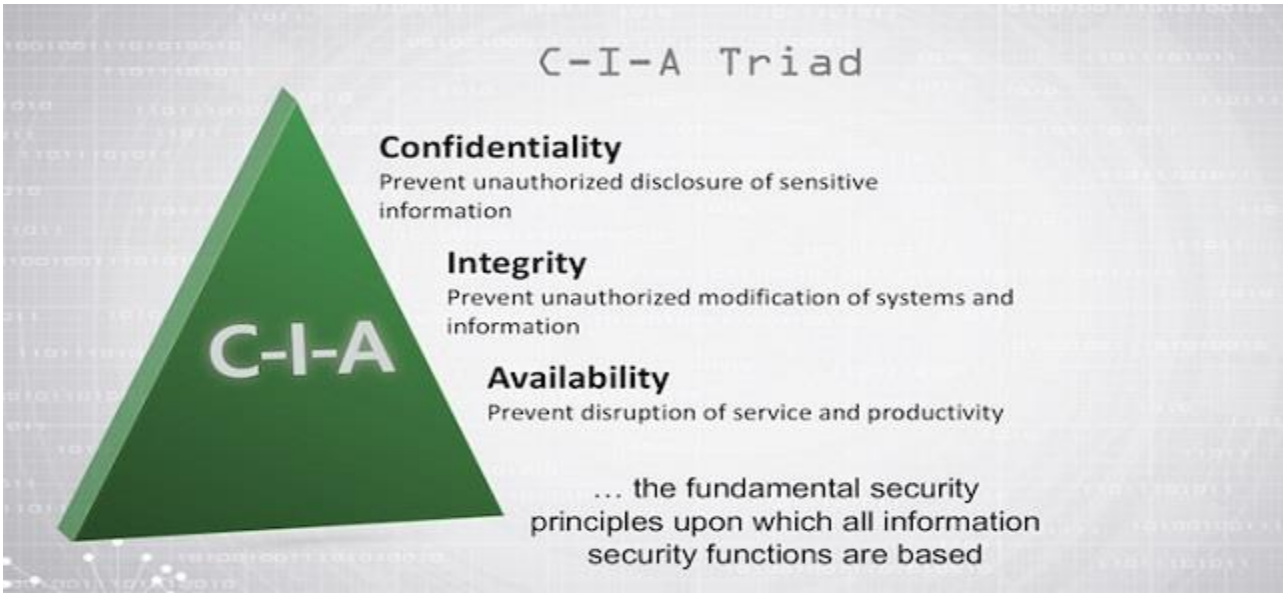
Unit VII: E-Security Systems

Information System Security:

Information systems security, more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.



The Information Security Triad: Confidentiality, Integrity, Availability (CIA):

1. Confidentiality:

When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality. For example, federal law requires that universities restrict access to private student information. The university must be sure that only those who are authorized have access to view the grade records.

2. Integrity:

Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. Just as a person with integrity means what he or she says and can be trusted to consistently represent the truth, information integrity means information truly represents its intended meaning. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something. An example of this would be when a hacker is hired to go into the university's system and change a grade.

Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information.

3. Availability:

Information availability is the third part of the CIA triad. *Availability* means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe. Depending on the type of information, *appropriate timeframe* can mean different things. For example, a stock trader needs information to be available immediately, while a sales person may be happy to get sales numbers for the day in a report the next morning. Companies such as Amazon.com will require their servers to be available twenty-four hours a day, seven days a week. Other companies may not suffer if their web servers are down for a few minutes once in a while.

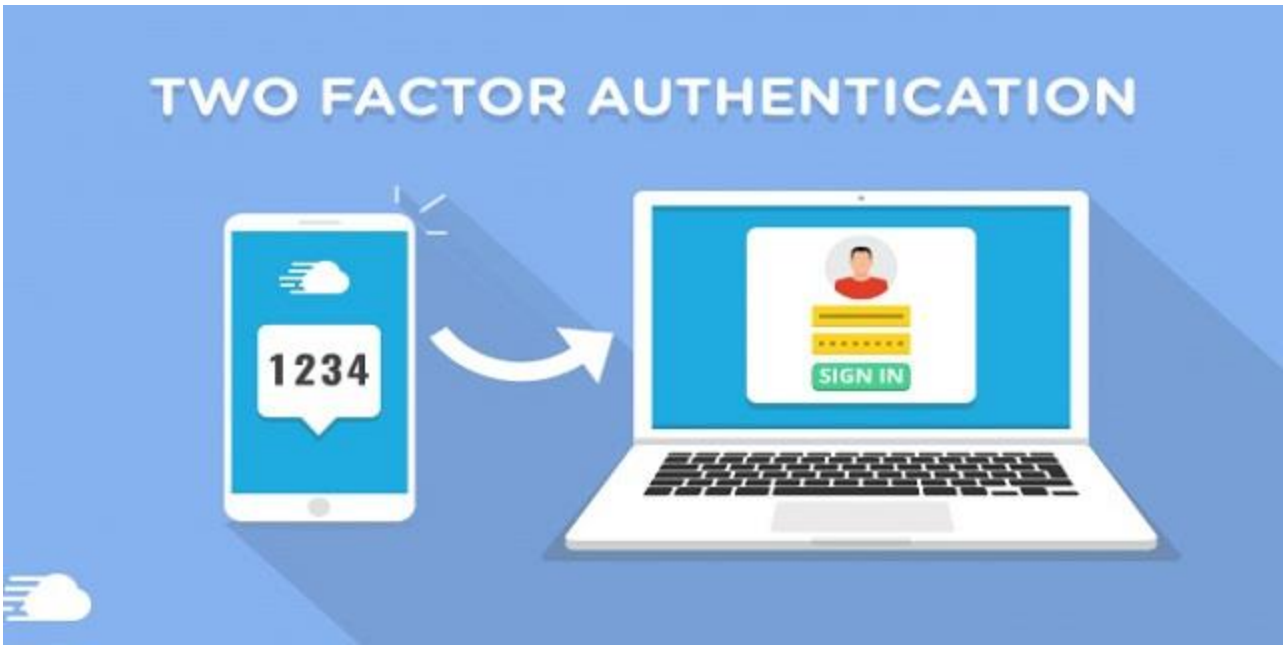
Tools for Information Security:

In order to ensure the confidentiality, integrity, and availability of information, organizations can choose from a variety of tools. Each of these tools can be utilized as part of an overall information-security policy.

1. Authentication:

The most common way to identify someone is through their physical appearance, but how do we identify someone sitting behind a computer screen or at the ATM? Tools for

authentication are used to ensure that the person accessing the information is, indeed, who they present themselves to be.



Authentication can be accomplished by identifying someone through one or more of three factors: **something they know, something they have, or something they are**. For example, the most common form of authentication today is the user ID and password. In this case, the authentication is done by confirming something that the user knows (their ID and password). But this form of authentication is easy to compromise and stronger forms of authentication are sometimes needed. Identifying someone only by something they have, such as a key or a card, can also be problematic. When that identifying token is lost or stolen, the identity can be easily stolen. The final factor, something we are, is much harder to compromise. This factor identifies a user through the use of a physical characteristic, such as an eye-scan or fingerprint. Identifying someone through their physical characteristics is called biometrics.

A more secure way to authenticate a user is to do multi-factor authentication. By combining two or more of the factors listed above, it becomes much more difficult for someone to misrepresent themselves. An example of this would be the use of an RSA Secure-ID token. The RSA device is something we have, and will generate a new access code every sixty seconds. To log in to an information resource using the RSA device, we combine something

we know, a four-digit PIN, with the code generated by the device. The only way to properly authenticate is by both knowing the code and having the RSA device.

2. Access Control:

Once a user has been authenticated, the next step is to ensure that they can only access the information resources that are appropriate. This is done through the use of access control. Access control determines which users are authorized to read, modify, add, and/or delete information. Several different access control models exist. Here we will discuss two**: the access control list (ACL) and role-based access control (RBAC).**

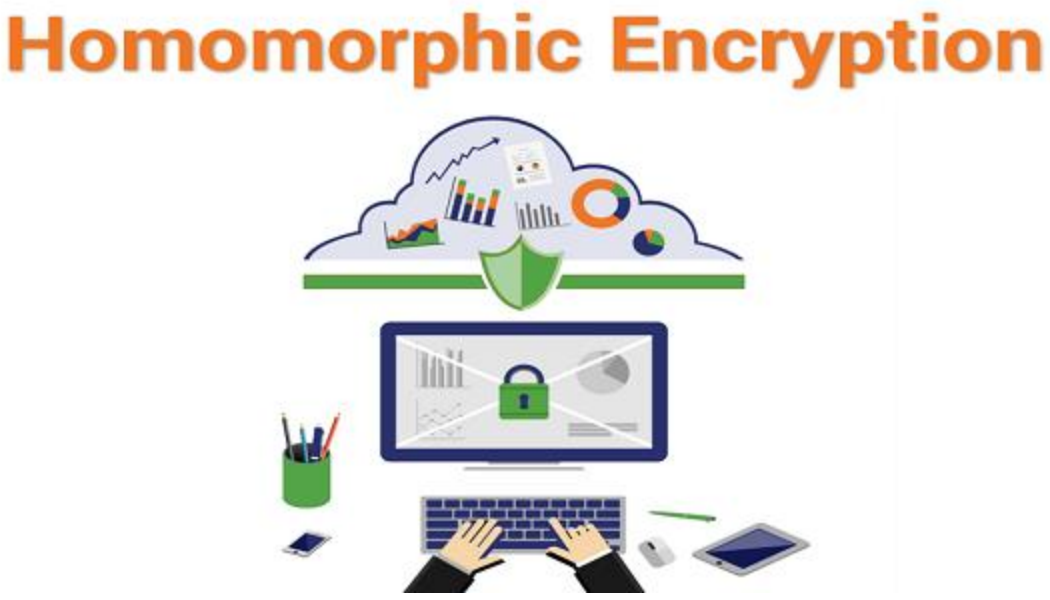
For each information resource that an organization wishes to manage, a list of users who have the ability to take specific actions can be created. This is an access control list, or ACL. For each user, specific capabilities are assigned, such as **read, write, delete, or add**. Only users with those capabilities are allowed to perform those functions. If a user is not on the list, they have no ability to even know that the information resource exists.

ACLs are simple to understand and maintain. However, they have several drawbacks. The primary drawback is that each information resource is managed separately, so if a security administrator wanted to add or remove a user to a large set of information resources, it

would be quite difficult. And as the number of users and resources increase, ACLs become harder to maintain. This has led to an improved method of access control, called **role-based access control, or RBAC**. With RBAC, instead of giving specific users access rights to an information resource, users are assigned to roles and then those roles are assigned the access. This allows the administrators to manage users and roles separately, simplifying administration and, by extension, improving security.

3. Encryption:

Many times, an organization needs to transmit information over the Internet or transfer it on external media such as a CD or flash drive. In these cases, even with proper authentication and access control, it is possible for an unauthorized person to get access to the data. Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it. This encoding is accomplished by a computer program, which encodes the plain text that needs to be transmitted; then the recipient receives the cipher text and decodes it (decryption). In order for this to work, the sender and receiver need to agree on the method of encoding so that both parties can communicate properly. Both parties share the encryption key, enabling them to encode and decode each other's messages. This is called **symmetric key encryption**. This type of encryption is problematic because the key is available in two different places.



An alternative to symmetric key encryption is **public key encryption**. In public key encryption, two keys are used: a public key and a private key. To send an encrypted message, we obtain the public key, encode the message, and send it. The recipient then uses the private key to decode it. The public key can be given to anyone who wishes to send the recipient a message. Each user simply needs one private key and one public key in order to secure messages. The private key is necessary in order to decrypt something sent with the public key.

4. Password Security:

Good password policies must be put in place, in order to ensure that passwords cannot be compromised. Below are some of the more common policies that organizations should put in place.

A. Require Complex Passwords:

One reason passwords are compromised is that they can be easily guessed. A recent study found that the top three passwords people used in 2012 were *password*, *123456* and *12345678*. A password should not be simple, or a word that can be found in a dictionary. One of the first things a hacker will do is try to crack a password by testing every term in the dictionary! Instead, a good password policy is one that requires the

use of a minimum of eight characters, and at least one upper-case letter, one special character, and one number.

B. Change Passwords Regularly:

It is essential that users change their passwords on a regular basis. Users should change their passwords every sixty to ninety days, ensuring that any passwords that might have been stolen or guessed will not be able to be used against the company.

C. Train Employees Not To Give Away Passwords:

One of the primary methods that is used to steal passwords is to simply figure them out by asking the users or administrators. Pretexting occurs when an attacker calls a helpdesk or security administrator and pretends to be a particular authorized user having trouble logging in. Then, by providing some personal information about the authorized user, the attacker convinces the security person to reset the password and tell him what it is. Another way that employees may be tricked into giving away passwords is through e-mail phishing. Phishing occurs when a user receives an e-mail that looks as if it is from a trusted source, such as their bank, or their employer. In the e-mail, the user is asked to click a link and log in to a website that mimics the genuine website and enter their ID and password, which are then captured by the attacker.

5. Backups:

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up. A good backup plan should consist of several components.

A. A Full Understanding Of The Organizational Information Resources:

What information does the organization actually have? Where is it stored? Some data may be stored on the organization's servers, other data on users' hard drives, some in the cloud, and some on third-party sites. An organization should make a full inventory of all information that needs to be backed up and determine the best way back it up.

B. Regular Backups Of All Data:

The frequency of backups should be based on how important the data is to the company, combined with the ability of the company to replace any data that is lost. Critical data should be backed up daily, while less critical data could be backed up weekly.

C. Offsite Storage Of Backup Data Sets:

If all of the backup data is being stored in the same facility as the original copies of the data, then a single event, such as an earthquake, fire, or tornado, would take out both the original

data and the backup! It is essential that part of the backup plan is to store the data in an offsite location.

D. Test Of Data Restoration:

On a regular basis, the backups should be put to the test by having some of the data restored. This will ensure that the process is working and will give the organization confidence in the backup plan.

Besides these considerations, organizations should also examine their operations to determine what effect downtime would have on their business. If their information technology were to be unavailable for any sustained period of time, how would it impact the business?

Additional concepts related to backup include the following:

A. Universal Power Supply (UPS):

A UPS is a device that provides battery backup to critical components of the system, allowing them to stay online longer and/or allowing the IT staff to shut them down using proper procedures in order to prevent the data loss that might occur from a power failure.

B. Alternate Or "Hot" Sites:

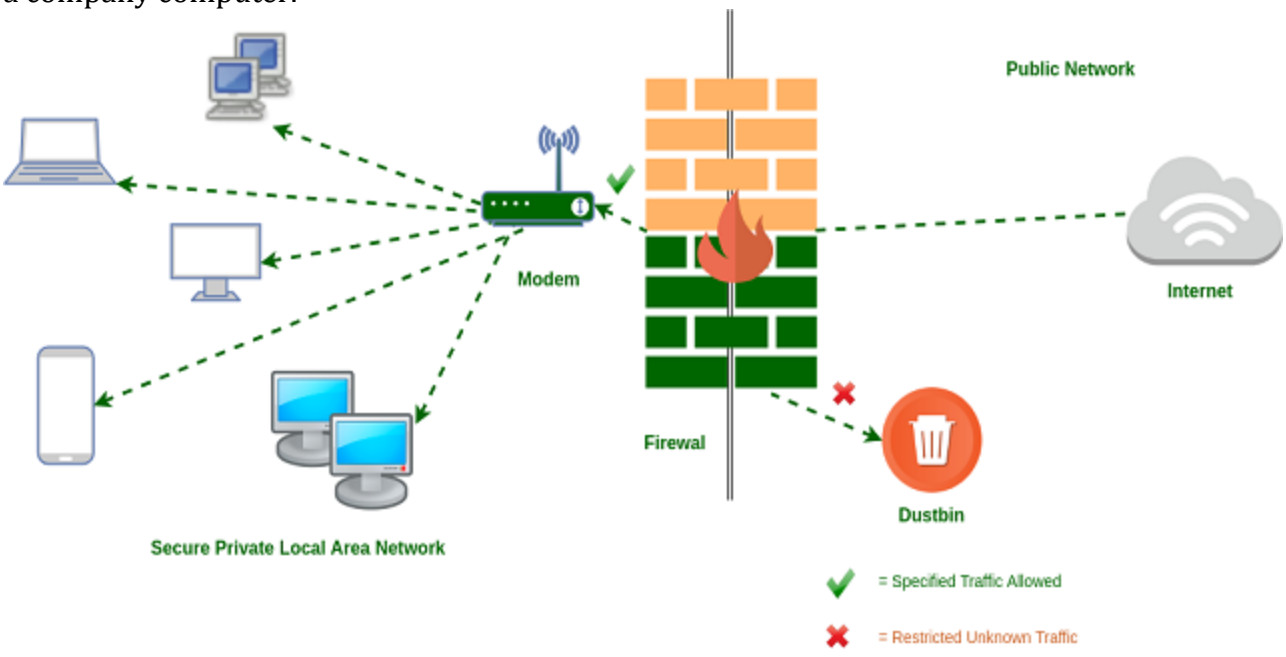
Some organizations choose to have an alternate site where an exact replica of their critical data is always kept up to date. When the primary site goes down, the alternate site is immediately brought online so that little or no downtime is experienced.

As information has become a strategic asset, a whole industry has sprung up around the technologies necessary for implementing a proper backup strategy. A company can contract with a service provider to back up all of their data or they can purchase large amounts of

online storage space and do it themselves. Technologies such as storage area networks and archival systems are now used by most large businesses.

6. Firewalls:

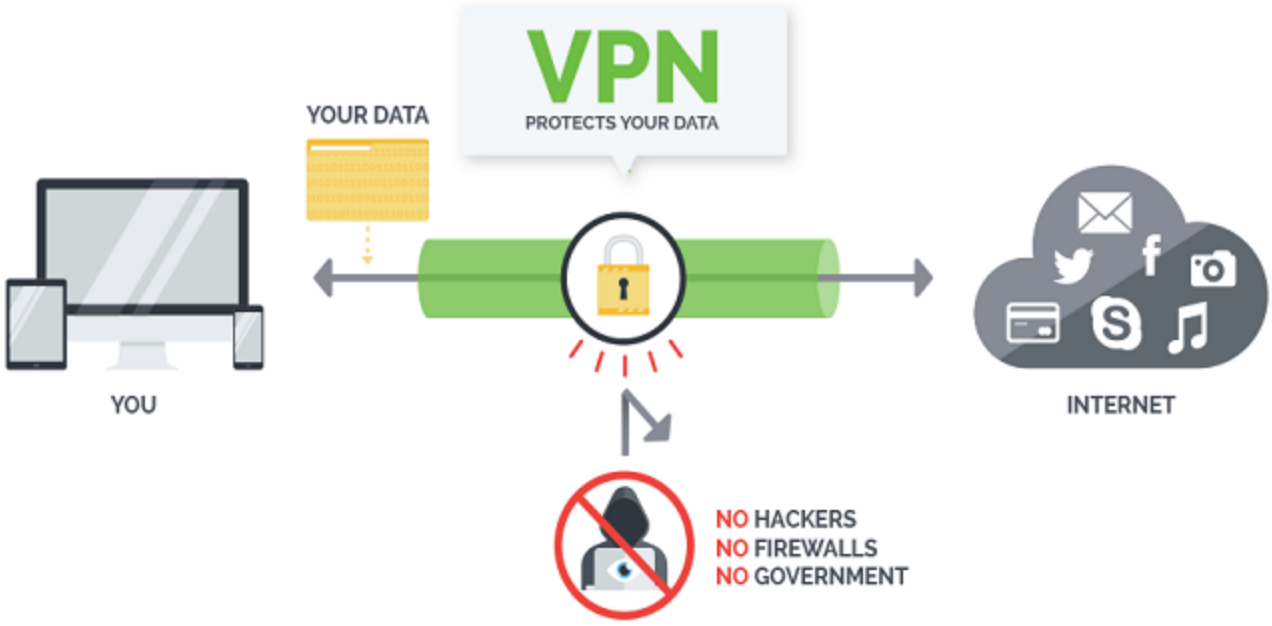
Another method that an organization should use to increase security on its network is a firewall. A firewall can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a computer. A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.



Some organizations may choose to implement multiple firewalls as part of their network security configuration, creating one or more sections of their network that are partially secured. This segment of the network is referred to as a DMZ, borrowing the term *demilitarized zone* from the military, and it is where an organization may place resources that need broader access but still need to be secured.

7. Virtual Private Networks:

Using firewalls and other security technologies, organizations can effectively protect many of their information resources by making them invisible to the outside world. But what if an employee working from home requires access to some of these resources? What if a consultant is hired who needs to do work on the internal corporate network from a remote location? In these cases, a virtual private network (VPN) is called for.



A VPN allows a user who is outside of a corporate network to take a detour around the firewall and access the internal network from the outside. Through a combination of software and security measures, this lets an organization allow limited access to its networks while at the same time ensuring overall security.

8. Physical Security:

An organization can implement the best authentication scheme in the world, develop the best access control, and install firewalls and intrusion prevention, but its security cannot be complete without implementation of physical security. Physical security is the protection of the actual hardware and networking components that store and transmit information

resources. To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically tampered with or stolen.

These measures include the following.

A. Locked Doors:

It may seem obvious, but all the security in the world is useless if an intruder can simply walk in and physically remove a computing device. High-value information assets should be secured in a location with limited access.

B. Physical Intrusion Detection:

High-value information assets should be monitored through the use of security cameras and other means to detect unauthorized access to the physical locations where they exist.

C. Secured Equipment:

Devices should be locked down to prevent them from being stolen. One employee's hard drive could contain all of your customer information, so it is essential that it be secured.

D. Environmental Monitoring:

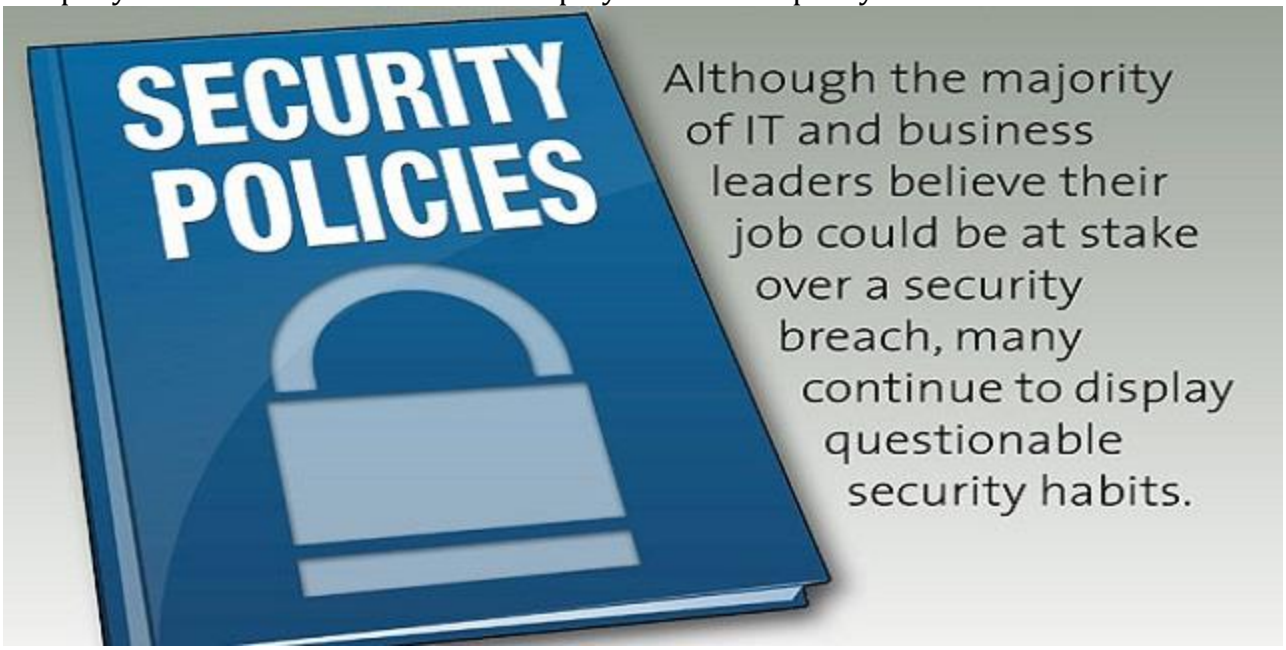
An organization's servers and other high-value equipment should always be kept in a room that is monitored for temperature, humidity, and airflow. The risk of a server failure rises when these factors go out of a specified range.

E. Employee Training:

One of the most common ways thieves steal corporate information is to steal employee laptops while employees are traveling. Employees should be trained to secure their equipment whenever they are away from the office.

9. Security Policies:

Besides the technical controls listed above, organizations also need to implement security policies as a form of administrative control. In fact, these policies should really be a starting point in developing an overall security plan. A good information-security policy lays out the guidelines for employee use of the information resources of the company and provides the company recourse in the case that an employee violates a policy.



According to the SANS Institute, a good policy is "a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area." Policies require compliance; failure to comply with a policy will result in disciplinary action. A policy does not lay out the specific technical details, instead it focuses on the desired results. A security policy should be based on the guiding principles of confidentiality, integrity, and availability.

A good example of a security policy that many will be familiar with is a web use policy. A web use policy lays out the responsibilities of company employees as they use company resources to access the Internet.

A security policy should also address any governmental or industry regulations that apply to the organization. For example, if the organization is a university, it must be aware of the Family Educational Rights and Privacy Act (FERPA), which restricts who has access to student information. Health care organizations are obligated to follow several regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

10. Mobile Security:

Mobile devices can pose many unique security challenges to an organization. Probably one of the biggest concerns is theft of intellectual property. For an employee with malicious intent, it would be a very simple process to connect a mobile device either to a computer via the USB port, or wirelessly to the corporate network, and download confidential data. It would also be easy to secretly take a high-quality picture using a built-in camera.

When an employee does have permission to access and save company data on his or her device, a different security threat emerges: that device now becomes a target for thieves. Theft of mobile devices (in this case, including laptops) is one of the primary methods that data thieves use.

So what can be done to secure mobile devices? It will start with a good policy regarding their use. According to a 2013 SANS study, organizations should consider developing a mobile device policy that addresses the following issues: use of the camera, use of voice recording, application purchases, and encryption at rest, Wi-Fi auto connect settings, Bluetooth settings, VPN use, password settings, lost or stolen device reporting, and backup.

Security on the Internet:

Internet security is a branch of computer security that deals specifically with internet-based threats. These include hacking, where unauthorized users gain access to computer systems, email accounts or websites; viruses and other malicious software (malware), which can damage data or make systems vulnerable to other threats; and identity theft, where hackers steal personal details such as credit card numbers and bank account information. We can protect ourselves from these threats with strong internet security.

1. Check Social Privacy Settings:

If we have social accounts, those networks have a lot of information about us, and we might be surprised how much of it is visible to anybody on the Internet by default. That's why it is strongly recommend us to check our privacy settings: It's up to us to decide what information we want to share with complete strangers versus our friends or even nobody but us.

2. Don't Use Public Storages For Private Information:

Oversharing is not limited to social networks. Don't use online services that are meant for sharing information to store private data. For example, Google Docs isn't an ideal place to store a list of passwords, and Dropbox is not the best venue for our passport scans unless they are kept in an encrypted archive.

3. Evade Tracking:

When we visit a website, our browser discloses a bunch of stuff about us and our surfing history. Marketers use that information to profile us and target us with ads. Incognito mode can't really prevent such tracking; we need to use special tools.

4. Keep Main E-Mail Address And Phone Number Private:

Our reward for sharing our e-mail address and phone number? Tons of spam in our e-mail inbox and hundreds of robocalls on our phone. Even if we can't avoid sharing this information with Internet services and online stores, don't share it with random people on social networks. And consider creating a separate, disposable e-mail address and, if possible, a separate phone number for these cases.

Create an additional e-mail account and purchase an additional SIM card to use for online shopping and other situations that require sharing our data with strangers.

5. Use Messaging Apps With End-To-End Encryption:

Most modern messaging apps use encryption, but in many cases it's what they call encryption in transit messages are decrypted on the provider's side and stored on its servers. What if someone hacks those servers? Don't take that risk, choose end-to-end encryption that way, even the messaging service provider can't see our conversations.

a. Use a messaging app with end-to-end encryption. For example, WhatsApp;

b. Note that by default, Facebook Messenger, Telegram and Google Allo do not use end-to-end encryption. To enable it, manually start a secret chat.

6. Use Secure Passwords:

Using weak passwords to protect our private information is as good as shouting that information to passersby. It's nearly impossible to memorize long and unique passwords for all the services we use, but with a password manager we can memorize just one master password.

a. Use long (12 characters and more) passwords everywhere;

b. Use a different password for each service;

7. Secure Phone And Computer With Passwords Or Passcodes:

Our computers and phones store a lot of data we'd rather keep private, so protect them with passwords. These passwords don't have to be complicated and unique, but they should keep random people out. On mobile devices, do a bit better: six-digit PINs or actual passwords rather than four digits and screen-lock patterns. For devices that support biometric authentication, whether fingerprint reading or face unlock, that's generally OK, but remember that these technologies have limitations. Use passwords or biometric authentication to lock phones, tablets, and computers.

8. Review Permissions For Mobile Apps And Browser Extensions:

Mobile apps prompt to give them permissions to access contacts or files in device storage, and to use the camera, microphone, geolocation, and so on. Some really cannot work without these permissions, but some use this information to profile us for marketing (and worse). Fortunately, it's relatively easy to control which apps are given which permissions. The same stands for browser extensions, which also have unfortunate spying tendencies.

9. Disable Lock Screen Notifications:

Protect phone with a long, secure password, but leave notifications on the lock screen? Now any passerby can see our business. To keep that information from appearing on the locked screen, set up notifications correctly.

10. Stay Private On Wi-Fi Networks:

Public Wi-Fi networks usually do not encrypt traffic, and that means anyone on the same network can try to snoop on our traffic. Avoid transmitting any sensitive data like logins, passwords, credit card data, and so forth over public Wi-Fi, and use a VPN to encrypt data and protect it from prying eyes.

a. Avoid using public Wi-Fi if possible;

b. If we connect to a public hotspot, use a secure VPN connection.

Network and Website Security Risks:

It is another requirement that the management should be familiar with the network and website security risks. Initially, the hacker was a term used to describe gifted software programmers while today, it refers to someone who deliberately gains unauthorized access to individual computers or computer networks.

Ethical hackers use their skills to find weaknesses in computer systems and make them known, without regard for personal gain. Malicious hackers, also called crackers, gain access to steal valuable information such as credit card numbers, attempt to disrupt service, or cause any other damage.

For secure business transactions in the network, an e-business must protect itself against such

a. Unauthorized access to its computer network,

b. Denial-of-service traffic overloads, and

c. The intrusion of destructive viruses.

Network Security Risks:

Nowadays cyber-threats are becoming a daily headache for IT security staff, it supports to have some guidance, or at least identify what to look out for. As a small company doing business on the web, we need to be aware of these methods so we can be extra vigilant when online. All the threat has been divided into three parts **internal threat, system threat and external threat** which is described below.

1. Internal Threat:

Internal threat is the threat that originating inside the corporation and commonly an exploit by a dissatisfied employee denied promotion or informed of employee termination.

The following are the possible internal threats that affect our organization:

a. Employee Theft:

Employee theft can be characterized as any stealing, utilize or abuse of business benefit without permission.

Security Measure:

i. Using a biometric identification system.
ii. Secretly watching employee and encourage them to own their success.

b. Weak Access Control:

Weak access control means the system is very weedy in a 3A (Authentication, Authorization, Accounting) security model and security process that controls use of particular assets inside of a predefined criteria.

Security Measure:

i. Strong password system with sufficient length to expand the difficulty it takes to split the password and they should be stored in the encrypted format.
ii. Making strong access control model policies (confidentiality, accountability, and integrity).

c. Privilege Abuse:

The peoples with rights who have extensive access to the resources of an organization might abuse it to satisfy their requirements or to destroy the organization reputation.

Security Measure:

i. Performs thorough background checks before issuance of privilege credentials.
ii. Bearing regular privilege user training.

2. System Threat:

The threat that harm physical equipment, hardware and system of organization is system threat.
The possible system threats to organizations are:

a. Equipment Failure:

Equipment failure refers to any occasion in which any equipment can't complete its intended task or reason. It can also mean that the hardware has stopped working.

Security Measure:

i. Regularly checking and maintenance of the physical equipment.

b. Power Fluctuation:

It refers to power surges and spikes which causes the electronic equipment to fail.

Security Measure:

i. Proper wiring and grounding of electronic equipment.
ii. Installing surge protector.

3. External Threat:

A threat that originating outside the organization or institution to the intention of damage or steal confidential information of that organization.
The possibly external threat for organization are listed below:

a. Malicious Threat:

Malicious threat include Computer viruses, Trojan, worm and spyware. It is code or software that is particularly intended to damage, steal, disrupt, or as a rule inflict some other "terrible" or illegitimate activity on information, hosts, or network.

Security Measure:

i. Install antivirus software into the system and download updates to ensure that software has the latest fixes for new viruses, Trojans, worms and bots.
ii. Ensure that antivirus software can scan email and all the files downloaded from the internet.

b. DOS attack:

A Denial-of-Service (DOS) attack is an attack intended to close down a machine or network, making it unavailable to its intended users.

Security Measure:

i. Using Over-provisioning brute force defence.
ii. Configuring windows firewall and IP access lists.

c. Eavesdropping:

Eavesdropping refers to the unauthorized monitoring of other people's communications. It can be conducted on ordinary telephone systems, emails, instant messaging or other Internet services.

Security Measure:

i. An electronic search of the radio frequency (RF) spectrum to detect any unauthorized emanations from the area being examined.
ii. Use encrypted data using data transmission or conversation.

d. Data Breaches:

A data breach is an occurrence in which sensitive, secured or confidential data has potentially been seen, stolen or utilized by an individual unapproved to do as such. In the case of small organization data breaches may involve personal information and intellectual property.

Security Measure:

i. Encrypting all the sensitive information and shred them before disposing.
ii. Retain the third party and limiting the staffs to access system and devices.

e. Phishing:

Phishing is the process to gain sensitive information like usernames, passwords and credit card information, frequently for malicious reasons, by taking on the appearance of a dependable element in electronic correspondence.

Security Measure:

i. Keep websites certificates up to date so that users are assured the legitimacy of the websites.
ii. Educate users about the best practices that they should follow and observe when using Internet services.

f. D-DOS Attack:

A distributed Denial of Service (DDOS) attack is a challenge to make an online service inaccessible by overpowering it with traffic from numerous sources. It focus on wide range banking information and confidential data of any organization.

Security Measure:

i. Limit the rate of router to prevent form web server being overwhelmed
ii. Use of firewall and pack sniffing technique for controlling high packet traffic

Website Security Risks:

1. Injection Flaws:

The top website security risks and vulnerabilities are injection flaws, particularly SQL injection flaws. According to OWASP, "Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query".

By employing injections, a hacker can trick our web application into executing unintended commands or accessing unauthorized data. A successful injection can result in a hacker gaining access to and changing, corrupting or deleting our data, denial of access, or even sometimes lead to complete host takeover.

The reason injections are considered the top risk is because once identified, they are very easily exploitable by a hacker.

2. Cross Site Scripting (XSS):

While injections are identified as the top risk, by far the most prevalent of website security risks is cross-site scripting.

"XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping." Cross site scripting can allow hackers to execute scripts in the victim's browser which can then allow them to hijack user sessions, deface our web site, or redirect our user to another (malicious) web site.

3. Broken Authentication and Session Management:

Authentication and session management functions are often not implemented correctly, which allows a hacker to compromise passwords, keys, session tokens, or exploit other website implementation flaws to assume a real website user's identity.

Where present, authentication and session management flaws may put all accounts at risk of an attack. Once successful, the hacker can do anything the victim has authorization to do view or do.

4. Insecure Direct Object References:

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without a proper access control check or other protection, hackers can find and manipulate these references to access unauthorized data.

5. Cross Site Request Forgery (CSRF):

"A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application." This allows the hacker to force the victim's browser to generate requests our website application believes are legitimate requests from the victim.

6. Security Misconfiguration:

Security misconfigurations often occur beyond simply our website application. "Good security requires having a secure configuration defined and deployed for the application,

frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application."

Indeed many of these misconfigurations may not even be things we have direct control over; for example, they are risks arising from our website hosting configuration.

7. Insecure Cryptographic Storage:

According to OWASP, "Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes."

8. Failure to Restrict URL Access:

This is another often insidious website security risk that goes unnoticed. "Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway."

9. Insufficient Transport Layer Protection:

"Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly."

10. Invalidated Redirects and Page Forwards:

The last of the top 10 website security risks (but by no means the last of the security vulnerabilities that may be present on our website) are invalidated redirects and page forwards.

Security Incidents on the Internet:

At recent times, distributed systems based on the client/server model have become common. There is an increase in the development and the use of distributed sniffers, scanners, and denial-of-service tools. Attacks using these tools can involve a large number of sites simultaneously and focus to attack one or more victim hosts or networks.

One incident could be a typical distributed attack system, in which the "**intruder"** controls a small number of **"masters**", which in turn control a large number of "**daemons**". Intruders then command the master to issue requests to the daemons in its list to ***launch attacks, shut down gracefully, or even announce themselves to a new master server.*** It happens due to well-known vulnerabilities that are exploited during installation of daemons and thus leading to root privileges on the machines.

In multitasking computer operating systems, a ***daemon*** is a computer program that runs as a background process, rather than being under the direct control of an interactive user and performs a specified operation at predefined times or in response to certain events. Typical daemon processes include print spoolers, e-mail handlers, and other programs that perform administrative tasks for the operating system. For example, *syslogd* is the daemon that implements the system logging facility. For example, **send mail program** initially discovered for UNIX systems still contain persistent vulnerabilities.

Similarly, in another case, sites using free FTP server could be contaminated with Trojan horse that permits privileged access to server. Many sites rely on such free software available on the internet that eventually adds capability for logging and breaks the access control, and integrity of the network and resources.

Thirdly, the major problem is the access by intruders who break through the gateways and installed sniffer programs that are used to monitor network traffic for usernames and static passwords typed in by users to connect into the networked system thus leading to many security threats and losses.

Some of the major security issues that could lead to those incidents on the internet are as follows:

1. Weak Authentication:

Authentication is one method in which the system verifies the identity of the user and allows or disallows the access based on the credential details. *Weak & static passwords* on the internet can be cracked in a number of ways. The two most common methods are by cracking the encrypted form of the password and another is by monitoring communication channels for password packets.

2. Ease of Spying:

There are various methods through which a user may connect to a remote host such as through Telnet or FTP.If a user connects to his/her account on a remote host using Telnet or FTP, then the user's password travels across the Internet unencrypted or in plain text which means that anyone monitoring the connections for IP packets, containing username and password, could also use them to log into the remote system.

3. Ease of Spoofing:

Spoofing is the creation of TCP/IP packets using somebody else's IP address.The IP address of a host is presumed to be valid and is therefore trusted by TCP and UDP services. But using IP source routing, an attacker's host can pretend as a trusted host or a client. *IP source routing is an option that can be used to specify a direct route to a destination and return path back to the origin.*

A simple example of how the attacker's system can pretend as the trusted client of a particular server is as follows:

1. The attacker would change its host's IP address to match that of the trusted client.
2. The attacker would then construct a source route to the server that specifies the direct path the IP packets should take to the server and back to the attacker's host, using the trusted client as the last hop in the route to the server.

3. The attacker sends a client request to the server using the source route.
4. The server accepts the client's request as if it came directly from the trusted client, and returns a reply to the trusted client.
5. The trusted client, using the source route, forwards the packet on to the attacker's host.

E-Business Risk Management Issues:

Risk is a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action. Its occurrence is uncertain but if it occurs when there is a possibility that there may be some loss or damage.

An e-business should also manage its e-business risks as a business issue, not just as a technology issue. An e-business must consider the direct financial impact of immediate loss of revenue, compensatory payments, and future revenue loss from e-business risks such as;
a. Business interruptions caused by website defacement (vandalism) or denial-of-service attacks.
b. Litigation (Legal Action) and settlement costs over employees' inappropriate use of e-mail and the internet.
c. Product or service claims against items advertised and sold via a website
d. Web-related copyright, trademark, and patent infringement lawsuits, and
e. Natural or weather-related disasters.

1. Website Defacement:

A **website defacement** is an attack on a **website** that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a **web** server and replace the hosted **website** with one of their own. An e-business should put in place an effective risk management program that includes;

a. Network and website security and intruder detection programs

b. Antivirus protection

c. Firewalls

d. Sound security policies and procedures

e. Employee education

2. Risk Insurance:

Another important component of a risk management program is the transfer of risk via insurance. Some of the kinds of insurance coverage an e-business should consider when developing an effective risk management program is as shown in Table below:

E-Risk Insurance	**Coverage**
Computer Virus Transmission	Protect against losses that occur when employees open infected e-mail attachments or download virus-laden software.
Extortion and Reward	Responds to Internet extortion demands and/or pays regards to help capture saboteurs.
Unauthorized Access/ Unauthorized Use	Covers failure to protect against third party access to data and transactions
Specialized Network Security	Responds to breach of network security and resulting losses.
Media Liability	Protects against intellectual property infringement losses.
Patent Infringement	Covers defensive and offensive costs when battling over patent infringement issues.
Computer Server and Services Errors and Omissions	Protects e-businesses against liability for errors and omissions when their professional advice causes a client's financial loss.

3. Firewall:

An Internet firewall is a system or group of systems that enforces a security policy between an organization's network and the Internet. It determines which inside service may be

accessed from the outside and which outsiders are permitted access to the permitted inside services, and which outside services may be accessed by insiders.

For a firewall to be effective, all traffic to and from the Internet must pass through the firewall. Some of the benefits of the firewall are as follows;

a. Protects Against Vulnerable Services: Filters insecure services and thus reduces risks to hosts on the subnet.

b. Controls Access to Site Systems: Only some of the hosts can be made reachable from the outside network making server systems unavailable.

c. Concentrates Security: All or most modified software and additional security software could be located on the firewall systems as opposed to being distributed to many hosts.

d. Enhances Privacy: Hides the names, IP addresses and blocks other important information from being available to the internet hosts.

e. Provides Valuable Statistics About The Network Usage: Keep log for all the incoming and outgoing accesses to the internet passing through it.

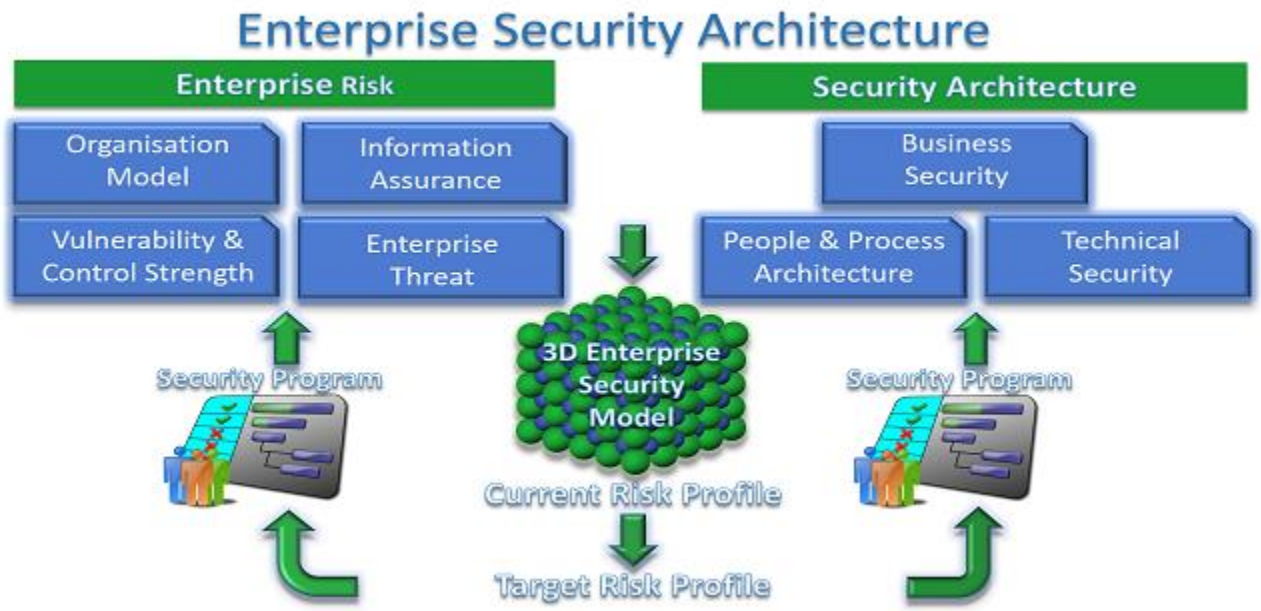
f. Provides Means For Policy Enforcement: It provides the means for implementing and enforcing a network access policy and thus controls users and services.

The most basic type of firewall is a **Packet Filter**. The packet filter firewall inspects each and every incoming and outgoing packet. Packets meeting some criterion described in rules formulated by the network administrator are forwarded normally and those that fail the test are dropped.

The other kind of firewall is the **Stateful firewall** which maps packets to connections and use TCP/IP header fields to keep track of connections. This allows for rules that, for example, allow an external Web server to send packets to an internal host, but only if the internal host first establishes a connection with the external Web server. *(Such a rule is not possible with stateless designs that must either pass or drop all packets from the external Web server).*

Another type is the **Application-Level Gateways.** It determines not only whether but how each connection through it is made. This type of firewall stops each incoming (or outgoing) connection at the firewall, and, if the connection is permitted, initiates its connection to the destination host on behalf of whoever created the initial connection.

Enterprise-Wide Security Framework:



Traditional Business Methods:

a. Policies and documents issued from the high-level directives provide a top-down influence
b. Policies were developed at one time in the organization's evolution to capture the current environment.

Major Challenges:

a. The continued growth and adaption of the policies to mirror the transformation within the organization.
b. Should incorporate security and protection of informational assets as new technology strategies such as intranets and extranets emerged.

Thus, they require newer technologies to maintain current technical environments. The first approach is to enforce the enterprise-wide information systems security policy as business needs change. Still, most companies implemented security policies to only some of the departments or individuals, but very little protection was provided to the enterprise as a whole. Thus the security policy should include three elements for the security policy – that is, **People, Policy and Technology**

a. People: Senior management, security administrators, systems and IT administrators, end-users, and auditors.

b. Policy: Security vision statement, security policy and standards, and the control documentation.

c. Technology: tools, methods, and mechanisms in place to support the process such as the operating systems, the databases, the applications, the security tools

The Security Framework:

The key elements, also referred to as the "Four Pillars" to information security, include;
Solid Senior Management Commitment
1. An overall Security Vision and Strategy
2. A comprehensive Training and Awareness Program
3. A solid Information Security Management Structure including key skill sets and documented responsibilities as shown in the figure.

Within The Four Pillars, Several Phases Are Included As:

1. Decision Drivers Phase:

The first phase - Decision Driver Phase contains factors determining the business derivers of security.It includes *Technology Strategy & Usage, Business Initiatives and Processes, and Threats, Vulnerabilities and Risk.*All these combine to form a unique "Security Profile" of the organization, which needs to be reflected in the Security Policies and Technical controls.

2. Design Phase:

The second phase include the Design of the security environment- i.e. the Design Phase.It is the phase in which the organization documents its security policy, the control environment and deals with controls on the technology level. It also defines the security model of the enterprise. Information classifications and risk assessment methods fall under this component.

3. Implementation Phase:

The last is the Implementation Phase which begins by documenting the Administrative and End-User guidelines and procedures, that should be flexible as per the changing environment. Enforcement, Monitoring, and Recovery processes are then layered on for the operational support of the security program.