# 7 E-Security System



### 7.1 Information System Security

Since all the transactions in e-businesses are made through public, it requires more concern on the network security.

The internet includes thousands of private computer networks and thus they are exposed to potential threats from anywhere around the public network,

This further leads for need to be secured from all such security threats so as to prevent data and information.



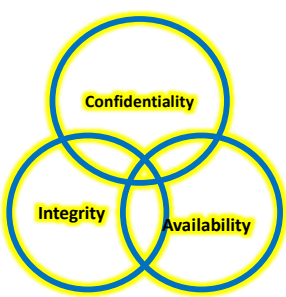
### 7.1 INFORMATION SYSTEM SECURITY

The major goals of security are;

i. Integrity of the data sent and received

ii. Confidentiality of the data so that it is not accessible to others

iii. The data ought to be available to the people for whom it is meant.




### 7.1 Information System Security

However, the requirement for sending information from source to destination without any tempering may be violated due to the followings.

a. Interruption of the data and cutting it off

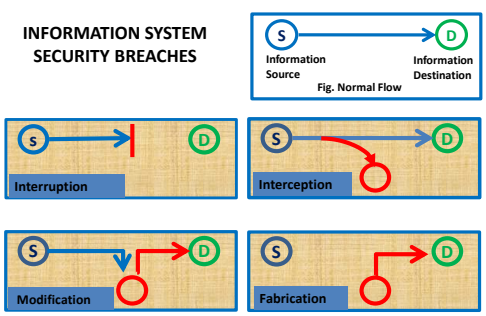
b. Interception of the data with the intent of spying on it

c. Interruption of the data and modify it, and send a different data to the receiver

d. Obstruct the data and fabricate new data and send it to the receiver



**INFORMATION SYSTEM SECURITY BREACHES**




### 7.1 Information System Security

The solution methods to prevent the occurrence of these problem are;

- Encryption
- Software Controls (access limitations in a data base, in OS; protect each user from other users)
- Hardware Controls (smartcard)
- Policies (frequent changes of passwords)
- Physical Controls

Besides these, e-businesses must also protect against any other unknown attacks.

## 7.1 Information System Security

**Information Security** is thus defined as ;

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

That is, it "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)."



## 7.1 Security on the Internet

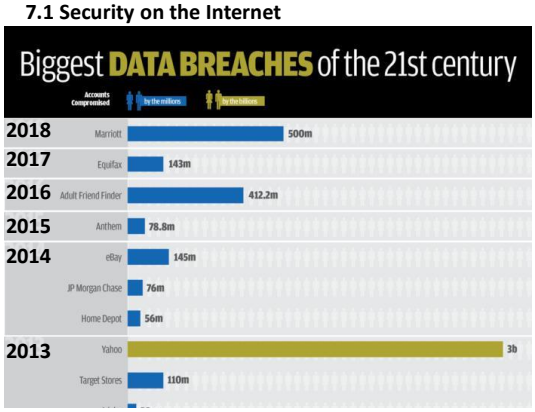
As the number of Internet users and the e-business is reaching its extremity, organization's private data and their network infrastructure are also being exposed to the crackers.

It has led to the requirement of the security policies to prevent unauthorized access to the private network resources as internet carries the network to the public.

Some of the security deficiencies that could result into inevitable break-ins in the network security are as follows;



## 7.1 Security on the Internet




## 7.1 Security on the Internet

Some of the ***security deficiencies*** that could result into inevitable break-ins in the network security are as follows;

**i. Vulnerable TCP/IP Services**

A number of TCP/IP services (like http, dhcp, smtp, etc) are not secure and can be compromised by knowledgeable intruders; services used in the local area networking environment for improving network management are especially vulnerable.

**ii. Ease of Spying and spoofing**

A majority of Internet traffic is unencrypted; e-mail, passwords, and file transfers can be monitored and captured using readily-available software. Intruders can then reuse passwords to break into systems.



## 7.1 Security on the Internet

**iii. Lack of Policy**

Many sites are configured unintentionally for wide-open Internet access, without regard for the potential for abuse from the internet;

Many sites permit more TCP/IP services than they require for their operations, and do not attempt to limit access to information about their computers that could prove valuable to intruders.

**iv. Complexity of configuration**

Host security access controls are often complex to configure and monitor; controls that are accidentally misconfigured often result in unauthorized access.



## 7.1 Security on the Internet

Due to the security vulnerabilities, business organizations at recent times have more to lose if the sites are hacked, as more of them depend on the internet for communication, operation and research.

The problems that could arise in the Internet and the factors that contribute to these problems are as follows:

**i. How secure is the server software ?**

- Prevent any unauthorized remote logon to the system.
- It should be extremely difficult to make changes to the server software.
- The servers themselves should be physically located in a secure environment.

## 7.1 Security on the Internet

**ii. How secure are communications ?**

Customer credit card information and other sensitive data that is being transmitted across the internet must be protected.

**iii. How is the data protected once it is delivered to the e-business?**

Is it stored in unencrypted text files at the website? Is it moved to offline storage?

**iv. How are credit card transactions authenticated and authorized ?**

Credit card transactions must be authenticated and authorized so as to make it more secure for the users.



## 7.1 Security on the Internet

Thus the general security issues that e-business must consider are;

| ISSUE | COMMENT |
|---|---|
| **Connection to the Internet** | Private computer networks are at risk from potential threats from anywhere on the public internet network |
| **Unknown Risks** | New security holes and methods of attacking networks are being discovered with alarming frequency |
| **Customer privacy and security of customer information** | Not only must steps be taken to protect the privacy of customer information, but also customers must be made aware of those steps and have confidence in them |
| **Security consciousness** | Management employees must understand the importance of security policies and procedures |



## 7.2 Network and Website Security Risks

It is another requirement that the management should be familiar with the network and website security risks.

Initially, 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.



## 7.2 Network and Website Security Risks

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

- unauthorized access to its computer network,
- denial-of-service traffic overloads, and
- the intrusion of destructive viruses.



## 7.2 Network and Website Security Risks

### Threats example;

One serious case is the denial-of-service attack, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries.

In 1999, a Swedish cracker broke into Microsoft's Hotmail Web site and created a mirror site that allowed anyone to type in the name of a Hotmail user and then read all of the person's current and archived email.



## 7.2 Network and Website Security Risks

### Threats

In another case, a 19-year-old Russian cracker named Maxim broke into an e-commerce Web site and stole 300,000 credit card numbers.

He then approached the site owners and told them that if they did not pay him $100,000, he would post all the credit card numbers to the internet. They did not give in to his blackmail, and he indeed posted the credit card numbers, inflicting great damage on many innocent victims.

### 7.2 Network and Website Security Risks

**Phishing**

Phishing scams are fraudulent attempts by cybercriminals to obtain private information. Phishing scams often appear in the guise of email messages designed to appear as though they are from legitimate sources.

Eg, the message would try to lure you into giving your personal information by pretending that your bank or email service provider is updating its website and that you must click on the link in the email to verify your account information and password details.



### 7.2 Network and Website Security Risks

**Denial-of-service Attacks (DoS)**

**DoS** attack is an attack on a network that is designed to disable the network by flooding it with useless traffic or activity.

A **Distributed Denial-of-Service (DDoS)** attack uses multiple computers to launch a Dos attack.

While a DoS attack does not do any technical damage it can do substantial financial damage to an e-business, because every second an e-business network or a website is down, it may result in loss revenues.



### 7.2 Network and Website Security Risks

**Denial-of-service Attacks (DoS)**

They do not affect the data on the websites, or

they cannot steal credit card numbers or proprietary information,

they cannot transfer money out of the bank account or

they cannot gain financially from these attacks,

however, they may result into loss of income or loss of reputation.



### 7.2 Network and Website Security Risks

**Distributed Denial-of-service Attacks (DDoS)**

In traditional DoS attack, the victim's computer might be able to figure out where the attack is coming from and shut down those connections, but in ***DDoS attack***, there is no single source and it's very complex to identify the attacker.



### 7.2 Network and Website Security Risks

**Spam**

Spam in the security context is primarily used to describe email spam - unwanted messages in your email inbox. Spam, or electronic junk mail, is a nuisance as it can clutter your mailbox as well as potentially take up space on your mail server.

Unwanted junk mail with advertising items may be harmless. However, spam messages may contain links that when clicked on could go to a website that installs malicious software onto your computer.



### 7.2 Network and Website Security Risks

**Viruses**

Viruses are the most common security risk faced by e-businesses today.

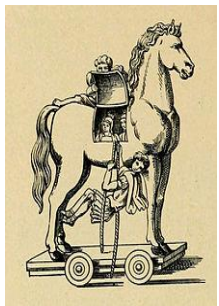
A virus is a small program that inserts itself into other program files that then become infected.

The virus is spread when an infected program is executed, and this further infects other programs.

Examples of virus effects include inability to boot, deletion of files or entire hard drives, inability to create or save files, and thousands of other possibilities.

## *Web Security*
## Threats – Trojan Horse

The **Trojan Horse** is a tale from the Trojan War about the trick that the Greeks used to enter the city of Troy and win the war. The Greeks constructed a huge wooden horse, and hid a selected force of men inside. The Greeks pretended to sail away, and the Trojans pulled the horse into their city as a victory trophy. That night the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greeks entered and destroyed the city of Troy, decisively ending the war.





### 7.2 Network and Website Security Risks

**Trojan Horse**

It has been named based on a real story and is a special type of virus that emulates a benign application.

It appears to do something useful or entertaining but actually does something else as well, such as destroying files or creating a "back door" entry point to give an intruder access to the system. A Trojan horse may be an e-mail in the form of attachment or a downloaded program.



### 7.2 Network and Website Security Risks

**Worm**

This type of virus does not directly alter program files. Instead, a worm replaces a document or an application with its own code and then uses that code to position itself.

Worms propagate by self-replication over a computer network.

Worms are often not noticed until their uncontrolled replication consumes system resources and slows down or stops the system.



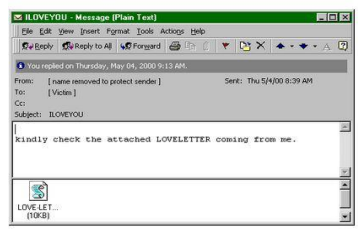
**Worm**

**3. ILOVEYOU – $15 Billion**

**Attachment**
**"LOVE-LETTER-FOR-YOU.TXT.vbs**

**Caused $15 billion in damages.**

**Arrived on and after May 4, 2000**




The virus was written by a college student.

Upon opening the attachment, the worm sent a copy of itself to everyone in the Windows Address Book and with the user's sender address.

This virus spread throughout the world in just a day, infecting computers of large corporations and governments, including the Pentagon in the United States.



### 7.2 Network and Website Security Risks

**Rogue security software**

Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe there is a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.



### 7.2 Network and Website Security Risks

**Adware**

Adware is unwanted software designed to throw advertisements up on your screen, most often within a web browser.

Typically, it uses an underhanded method to either disguise itself as legitimate, or attached on another program to trick you into installing it on your PC, tablet, or mobile device.

### 7.2 Network and Website Security Risks

**Spyware**

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.



### 7.2 Network and Website Security Risks

**Ransomware**

Ransom malware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

*67% of businesses attacked by ransomware have permanently lost part of or all of their company data. By infecting secure database systems, encrypting data, and threatening deletion or corruption of files unless a heavy ransom is paid, ransomware is a very dangerous form of malware.*



### 7 E-Security System

### 7.3 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.



### 7 E-Security System

### 7.3 Security Incidents on the Internet

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.



### 7 E-Security System

### 7.3 Security Incidents on the Internet

In multitasking computer operating systems, a ***daemon*** (/ˈdiːmən/ or /ˈdeɪmən/) 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.



### 7 E-Security System

### 7.3 Security Incidents on the Internet

For example,

**sendmail 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 in the internet that eventually adds capability for logging and breaks the access control, and integrity of the network and resources.

**7 E-Security System**

**7.3 Security Incidents on the Internet**

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.



**7 E-Security System**

**7.3 Security Incidents on the Internet**

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

**Weak Authentication**

Authentication is one method in which the system verifies 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.



**7 E-Security System**

**7.3 Security Incidents on the Internet**

**Ease of Spying**

There are various methods through which a user may connect to a remote host such as through Telnet or FTP.

**Guess what could happen, if it's an Administrator's Password ??**

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.



**7 E-Security System**

**7.3 Security Incidents on the Internet**

**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.*



**7 E-Security System**

**7.3 Security Incidents on the Internet**

**Ease of Spoofing**

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.



**7 E-Security System**

**7.3 Security Incidents on the Internet**

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.

**7 E-Security System**

## 7.4 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 then there is possibility that there may be some loss or damage.



**7 E-Security System**

## 7.4 E-Business Risk Management Issues

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;

- Business interruptions caused by website defacement (destruction) or denial-of-service attacks.

*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.*



**7 E-Security System**

## 7.4 E-Business Risk Management Issues

- Litigation (Legal Action) and settlement costs over employees' inappropriate use of e-mail and the internet
- Product or service claims against items advertised and sold via a website
- Web-related copyright, trademark, and patent violation lawsuits, and
- Natural or weather-related disasters.



**7 E-Security System**

## 7.4 E-Business Risk Management Issues

An e-business should put in place an effective risk management program that includes;

- Network and website security and intruder detection programs
- Antivirus protection
- Firewalls
- Sound security policies and procedures
- Employee education



**7 E-Security System**

## 7.4 E-Business Risk Management Issues

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 7.1



**7 E-Security System**

**Table 7.1 E-Risk Insurance**

| E-risk insurance | Coverage |
|---|---|
| **Computer Virus Transmission** | Protects 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(One who tries to conceal identity) |
| **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. |

**7 E-Security System**

**7.4 E-Business Risk Management Issues**


**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.



**7 E-Security System**

**7.4 E-Business Risk Management Issues**

**Firewall**

For a firewall to be effective, all traffic to and from the Internet must pass through the firewall.

Some of the benefits of firewall are as follows;

- *Protects against vulnerable services* - Filters insecure services and thus reduces risks to hosts on the subnet.
- *Controls access to site systems* - Only some of the hosts can be made reachable from the outside network making server systems unavailable.



**7 E-Security System**

**7.4 E-Business Risk Management Issues**

**Firewall**

- *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.
- *Enhances privacy* - Hides the names, IP addresses and blocks other important information from being available to the internet hosts.
- *Provides valuable statistics about the network usage* - Keep log for all the incoming and outgoing accesses to the internet passing through it.



**7 E-Security System**

**7.4 E-Business Risk Management Issues**

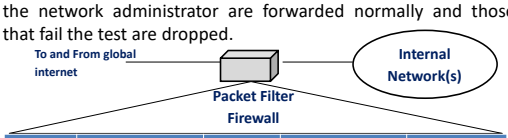
**Firewall**

- *Provides means for policy enforcement.* It provides the means for implementing and enforcing a network access policy and thus controls users and services.



**Firewall -**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 descried in rules formulated by the network administrator are forwarded normally and those that fail the test are dropped.




| Interface | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|
| 1 | 172.10.0.0 | * | * | * |
| 2 | * | * | * | 23 |
| 3 | * | * | 192.168.1.11 | * |
| 4 | * | 80 | * | * |



**Firewall**

In the previous figure, the following packets are filtered.

a. Incoming packets from network 172.10.0.0 are blocked. Here, '*' means "any".
b. Incoming packets destined for any internal TELNET server (port 23) are blocked.
c. Incoming packets destined for internal host 192.168.1.11 are blocked. The organization wants this host for internal use only.
d. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the internet.

## Firewall

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).*



## Firewall

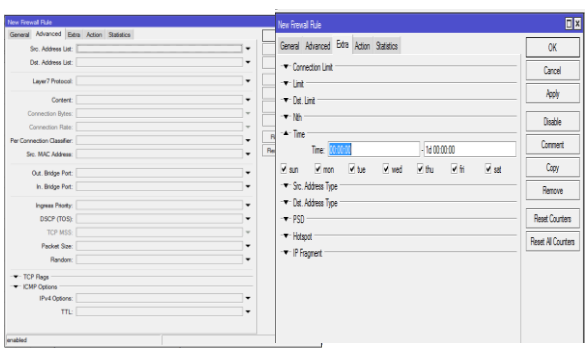
Another type is the **Application-Level Gateways.**

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.

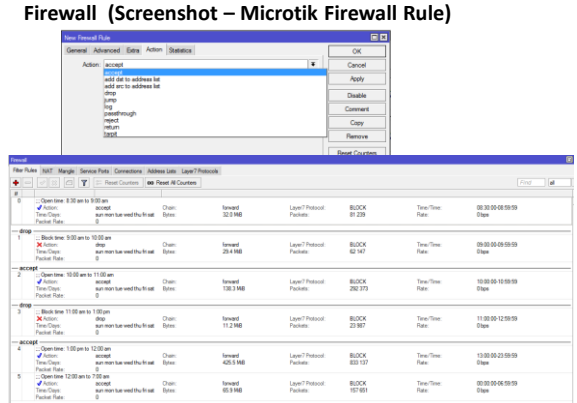


## Firewall (Screenshot – Microtik Firewall Rule)





## Firewall (Screenshot – Microtik Firewall Rule)



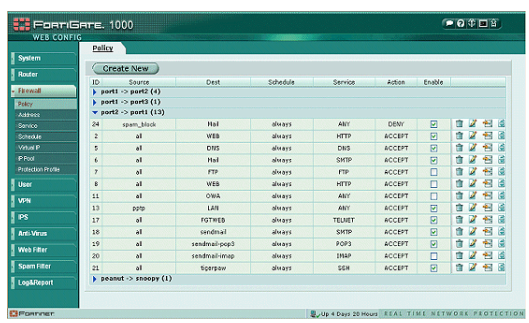
## Firewall (Screenshot – Microtik Firewall Rule)

**Firewall Rules Configuration**

| Active | Type | Rule | Protocol | Source | Port(s) | Destination | Port(s) | Comments |
|---|---|---|---|---|---|---|---|---|
| No | Access | Permit | UDP | IP or Host Name 192.168.0.50 | ALL | Any | 53 | Example - Permit DNS request to this IP |
| No | Access | Permit | TCP | IP or Host Name 192.168.0.50 | ALL | Any | 110 | Example - Permit POP access to this IP |
| No | Access | Permit | TCP | IP or Host Name 192.168.0.50 | ALL | Any | 25 | Example - Permit SMTP access to this IP |
| No | Access | Deny | ALL | IP or Host Name 192.168.0.50 | ALL | Any | ALL | Example - Deny all access to this IP |
| No | Access | Deny | ALL | IP or Host Name 192.168.0.48/30 | ALL | Any | ALL | Example - Deny access to this Sub-net |
| No | Access | Deny | TCP | Any | ALL | Any | 21 | Example - Deny access to FTP sites |



## Firewall (Screenshot – Fortigate Firewall Policy)



## 7 E-Security System

### 7.4 Enterprise-wide security Framework

**Traditional business methods**

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

**Major challenges**

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



## 7 E-Security System

### 7.4 Enterprise-wide security Framework

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** called the **PPT Model**



## 7 E-Security System

### 7.4 Enterprise-wide security Framework

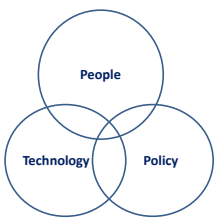



Fig. People, Policy and Technology

**People** – Senior management, security administrators, systems and IT administrators, end users, and auditors.

**Policy** - security vision statement, security policy and standards, and the control documentation.

**Technology** - tools, methods, and mechanisms in place to support the process, and this includes the operating systems, the databases, the applications, the security tools



## 7 E-Security System

### 7.4 Enterprise-wide security Framework

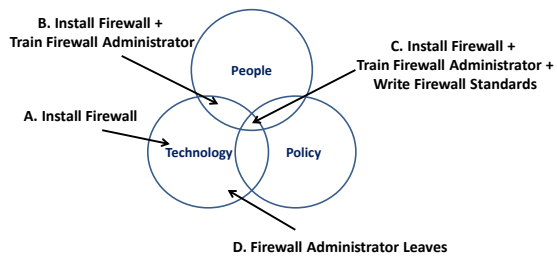



Fig. PPT Model – Internet Connection : coverage by three elements



## 7 E-Security System

### 7.4 Enterprise-wide security Framework

***The Security Framework***

The key elements, also referred to as the "Four Pillars" to information security, include;

1. Solid Senior Management Commitment
2. An overall Security Vision and Strategy
3. A comprehensive Training and Awareness Program
4. A solid Information Security Management Structure including key skill sets and documented responsibilities as shown in the figure.



## 7 E-Security System

### 7.4 Enterprise-wide security Framework

***The Security Framework***

Within the four pillars, several phases are included as;

I. Decision Drivers Phase,

II. Design Phase, and

III. Implementation Phase

## 7.4 Enterprise-wide security Framework

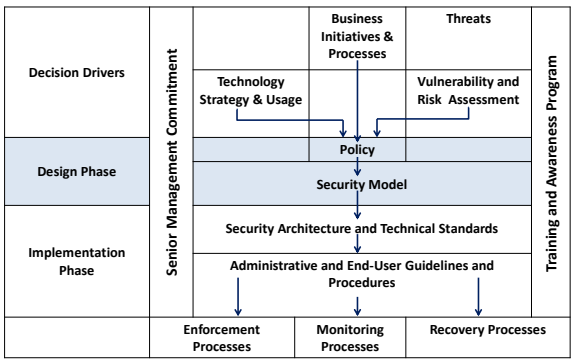



**Fig. Information Security Management Structure**



## 7 E-Security System

## 7.4 Enterprise-wide security Framework

***The Security Framework***

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.



## 7 E-Security System

## 7.4 Enterprise-wide security Framework

***The Security Framework***

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.



## 7 E-Security System

## 7.4 Enterprise-wide security Framework

***The Security Framework***

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.