


Introduction to Information Security
Prof. Dilip H. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 32

(Refer Time Slide: 00:10)

Module 3




- Vulnerability, Threat and Risk, Risk Assessment and Mitigation + Quick fixes, Introduction to BCP / DRP / Incident management, Segregation and Separation of Duties & Roles and responsibilities.

1

After an exciting session, from Dr Kamakoti, let us move on to module 3. Module 3 deals with vulnerability, threat, risk, risk assessment and mitigation, quick fixes, introduction to BCP, DRP, incident management, segregation and separation of duties, and roles and responsibilities.

(Refer Time Slide: 00:32)

Vulnerability, Threat, Risk

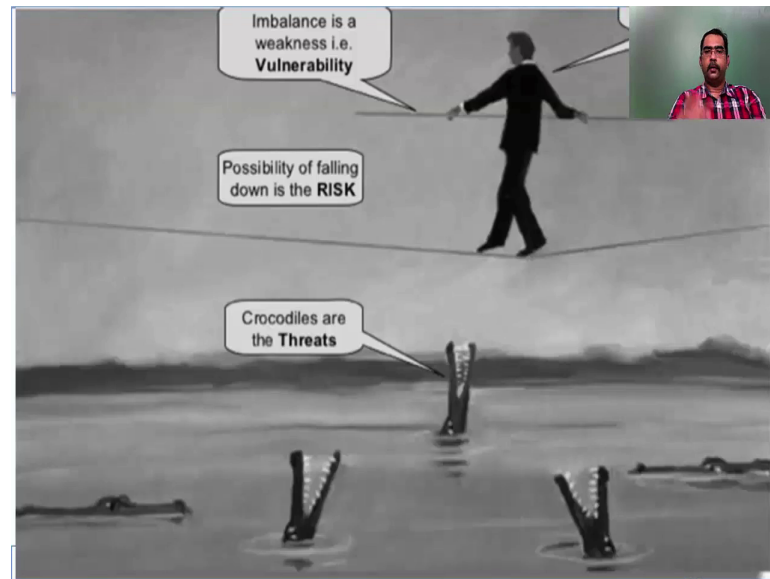


- “If you know the enemy and know yourself, you need not fear the result of a hundred battles.”
– Sun Tzu, Art of War

2

Sun tzu in his book, art of war stated if you know the enemy and know yourself, you need not fear the results of 100 battles, what it effectively means is, you should know what threats effect or organization, organization security, and how it will impact your organization. And if you make appropriate provisions, or appropriate security measures are implemented, then you need not a fear the result of 100 battles.

(Refer Time Slide: 01:06)




Now, let us take a look at this slide, this is a very clear definition of what vulnerability, threat, risk, and asset is, now if you see the image, you see that the person is the asset as in an organization, imbalance he is working on a tight rope. So, imbalance is a weakness, which is vulnerability. The crocodiles in the river down below are the threats and possibility of falling down is the risk. If you take a technical example, our computer system is the asset, not having a antivirus software is a vulnerability.

The virus attack itself is a threat, or likely hood of a virus attack is a threat, and possibility of your data being lost is the risk. let us move on.

(Refer Time Slide: 02:04)

A Quick Vocabulary Les



- Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that may result in a security breach or a violation of the system's security policy.

So, what is a vulnerability, let us take a look at the definition vulnerability is a flaw of weakness in the system security procedures, in the design, in the implementation, in internal controls, that may result in security breach, or a violation of system security policy. Now, this is a big definition, let us tell it in simple plain English, there is a hole in the system, it is a weakness in the system.

So, what you need to understand is, vulnerability is a hole or weakness in the system, where can the hole can be, it can be in policies, in procedures, in your technical implementations, in your internal controls. The vulnerability is simply, a hole or weakness in the system.

(Refer Time Slide: 02:51)

Vulnerabilities



- Where do they come from?
 - Flaws in software
 - Faulty configuration
 - Weak passwords
 - Human error
 - Inappropriately assigned permission levels
 - System inappropriately placed in infrastructure/environment
- Vulnerabilities don't go away by themselves

So, where do vulnerabilities come from, they come from various methods, flaws in the software. The software is not designed properly, not developed properly, does not meet the user requirement, faulty configuration, your servers or not configured properly. A data base is not configured properly, a network is not configured properly, it can come because of weak passwords not following minimum guide line for having a password.

Say minimum 8 characters is not implemented, no alpha numeric, special characters are validated, there is no system of periodically force changing the password. Then human error that is possibly the most important, and most common occurrences in any organization. An inappropriately assigned permission level, inadequately assigned permission level.

So, you have an organization where you need to assign the permission, on an need to know, need to do basis, but you have given more permissions to certain users, by which they can cause loss, or damages to the system. So, that is inappropriately assigned permission levels, and system inappropriately placed in the infrastructure, or environment. If we take an example, you have a critical server in your organization, you have big hall where a lot of people work there, your employees work there.

You take the server, and go put it on the middle of the hall. So, there is a likely hood which is not physically protected, it is not logically protected, no password policies are follow. So, what a basically will happen is, somebody can come pull out the network cable, pull out the power cable, they can log on to the system, they can just power off the system.

So, that means, system is inappropriately placed in the infrastructure, or environment and vulnerabilities they just do not go away by them self. So, once it is there, you will have to take adequate measures, or put in controls for the vulnerabilities to go away.

(Refer Time Slide: 05:06)



Threats

- A **threat** is any event, malicious or otherwise, that can have an undesirable effect on the assets and resources associated with a computer system or network.
 - Natural Disasters
 - System and component failures
 - Organizations or individuals who both intend us harm and have the capability to accomplish their intentions
 - Computer hackers, criminals, industrial or enemy armed forces, terrorists or saboteurs

6

Now, what is a threat in simple terms, threat is something which exploits the vulnerability, but the definition of a threat is it is, any event malicious or otherwise, that can have an undesirable effect on the assets. So, assets can be people, process or technology, and resources associated with the computer system, or network.

So, what are the resources associate with a computer system on to again people, process technology, a threat can be a natural disaster, fire flood, earthquake, tsunami, system and component failures. At this failure, we have memory failure, organizations are individuals who both intend us harm, and have the capability to accomplish their intentions like computer hackers, criminals or enemy, armed forces, terrorists or saboteurs. You have to include, internal employees also in to this, because a disgruntled employee is as bad for the organization, as an external hacker.

(Refer Time Slide: 06:17)

Threats (continued)



- Threats can affect
 - Confidentiality (“disclosure threat”)
 - Integrity (“alteration threat”)
 - Availability (“denial of service threat”)

So, what do threats effect, threats effect we are heard these 3 terminologies over and over again in module 1, threats effect confidentiality, integrity, availability of information and information resources, now the opposite of confidentiality is disclosure, integrity is alteration, and availability is destruction, or denial of service threat.

(Refer Time Slide: 06:43)

Threats



- Employees
- External Parties
- Low awareness of security issues
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Natural Disasters eg. fire, flood, earthquake

8

Let us look at some of example for threats, employees, external parties, low awareness of security issues, and growth in networking or distributed computing, growth in complexity and effectiveness of hacking tools and viruses, natural disasters. Now, employee why are they a threat? A disgruntled employee can always be a threat to the organization, because he can cause loss or damage to the system, if he is not satisfied with what he are doing.

You take an example you already gone through the example of logic bombs. So, employees are retrieving right, if the person says that, if my name does not appear in the pay roll in the subsequent month on the seventh, then dell dot dell star dot star on the system. So, that is the logic bomb. External parties, your are consultants, vendors, all the external people that an organization associates with or a risk, or a threat.

Low awareness of security issues. Why the emphasis is on low awareness security, awareness training should be an ongoing process for any organization it should not be one time affair. Every new employee, and employees who are already working in the organization, have to under go the security awareness training, on a routine basis, on a regular basis. Growth in networking and distributed computing. Now, the networks are grown over the last few years, to a very complex level.

Today, people talk about cloud, large networks, very large networks, but once upon a time the networks is to be confine to a probably a small lan, may be a small geographical area, now it is become large. So, you will have to deal with multiple threats, then growth in complexity, and effectiveness of hacking tools, and viruses. Again there are so many tools, which are available in a market today, which are fully automated to do a certain task.

For example, you have any expose, which is a vulnerability assessment tool, which can do an end to end network assessment, including a router, your firewalls, your servers, your desktops. So, the complexity and effectiveness of these tools have also got a very important role. So, that means if somebody can sit outside your network, and scan your network for the vulnerabilities, and find out what are the loop wholes is doing it, in a passive basis is not even coming, into your organization.

So, he gather information from outside, and then decides to launch a full scale attack. Then natural disasters is self explanatory, fire is a problem, flood is a problem, earthquake is a problem.

(Refer Time Slide: 09:41)

Threat Sources		
Source	Motivation	Threat
External Hackers	Challenge Ego Game Playing	System hacking Social engineering Dumpster diving
Internal Hackers	Deadline Financial problems Disenchantment	Backdoors Fraud Poor documentation
Terrorist	Revenge Political	System attacks Social engineering Letter bombs Viruses Denial of service
Poorly trained employees	Unintentional errors Programming errors Data entry errors	Corruption of data Malicious code introduction System bugs Unauthorized access

What are the threat sources, external hackers are a source, what is the motivation for an external hacker, it is a challenge, he has challenged some one that he is going to hack into x y z network. Ego is another factor, just to prove that we can hack into the network, and just play around. And what is the threat, the threat for the organizational system hacking social engineering, social engineering is the art of deception, or the art of trying to con the employees in to believing that, you are someone, and trying to gather as much information as possible, about the organization.

Dumpster diving means, you are going through, the trash cans are the garbage bins in the organization finding, if any confidential information is available. So, that you can use it for launching an attack later, then the source of threat is internal hackers, dead line is a problem I am not able to finish my job on deadlines. So, I need to bring down the system, so that I can blame the system for not finishing my job.

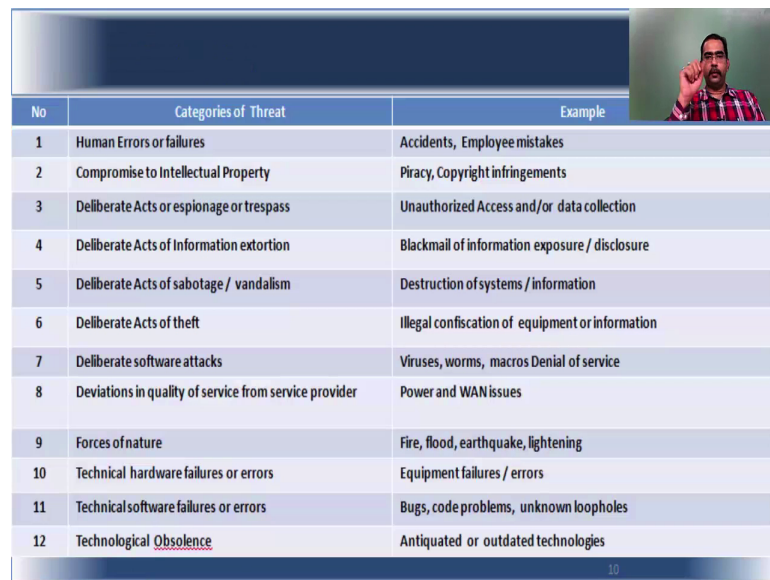
I can install a back door, for that. The financial problem is probably the biggest motivating factor. A fraud can be perpetuated or poor documentation. Your disassociated with whatever is happen. Terrorist activity, it can be a revenge or for political reasons, and different type of threats can come like system attacks, social engineering we already seen, letter bombs, we have read about it, the viruses and of course, denial of service, then poorly trained employee.

Probably this will be the most important thing again I am emphasizing, where lack of security awareness is probably, the biggest cause of security flaws or weaknesses which are found in the organizations. The employees can do unintentional errors, because they do not know, whether they are doing it right or not. It is not a intended to commit of

felony, or a fraud. Some programming errors may be not following secure coding practices, can lead to programming errors.

Again it is not deliberate it is, because of the lack of awareness. Data entry errors can happen to anyone, but again if they trained properly to verify, what they have enter, then the errors can be minimized, what is the threat of this corruption of data, malicious code introduction that is for programming. You can say back door is the example of malicious code introduction system bugs, and unauthorized access.

(Refer Time Slide: 12:36)



No	Categories of Threat	Example
1	Human Errors or failures	Accidents, Employee mistakes
2	Compromise to Intellectual Property	Piracy, Copyright infringements
3	Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
4	Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
5	Deliberate Acts of sabotage / vandalism	Destruction of systems / information
6	Deliberate Acts of theft	Illegal confiscation of equipment or information
7	Deliberate software attacks	Viruses, worms, macros Denial of service
8	Deviations in quality of service from service provider	Power and WAN issues
9	Forces of nature	Fire, flood, earthquake, lightening
10	Technical hardware failures or errors	Equipment failures / errors
11	Technical software failures or errors	Bugs, code problems, unknown loopholes
12	Technological <u>Obsolence</u>	Antiquated or outdated technologies

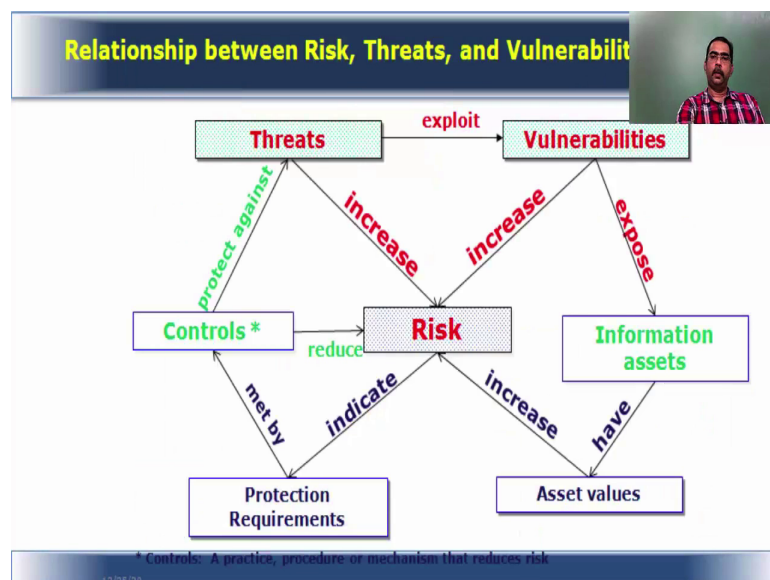
Let us see a few examples of categories of threat, and some example human errors, and failures employee's mistake is an example, accident some example for compromise to intellectual property, copyright infringements is an example, piracy of software is an example. Then espionage or trespass unauthorized access, to or data collection is an example. So, similarly there are around 12 items listed here for categories of thereat, and the corresponding examples.

(Refer Time Slide: 13:10)



Just to show you an graphical form, the same threats high user knowledge of IT system theft sabotage or misuse virus attacks are the threat lack, or lapse in. Physical security policy is a threat, natural calamities and fire is a threat, not having proper documentation is also a threat. If there is a failure in a communication line or a system, that is also a threat.

(Refer Time Slide: 13:38)



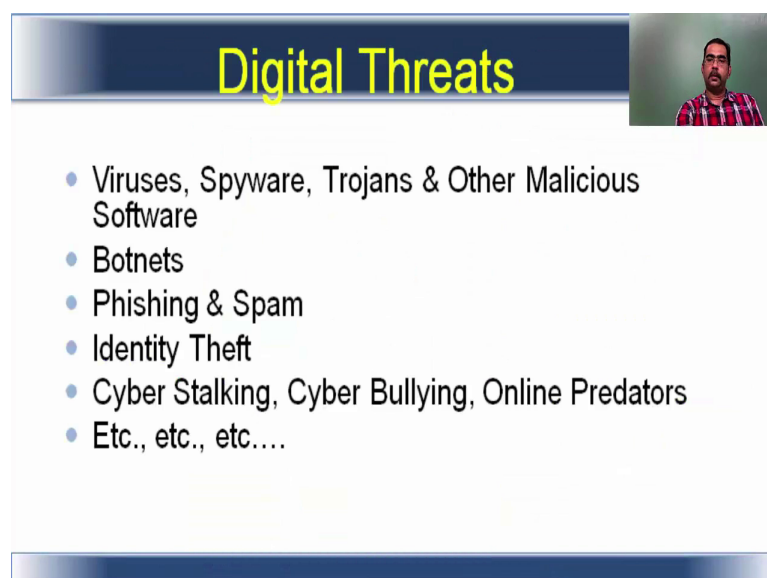
So, what is the relationship between vulnerabilities, threat and risk, you know that the basic thing is vulnerability, what exploits vulnerability, the threats exploit vulnerability. The vulnerabilities expose the information assets, vulnerability also increases risk, and threat also increases risks. So, when the asset is an asset value for that, so in the more the asset value, the higher the risk. Protection requirement indicate risk, if I am spending x

amount of money, then it means that I am trying to protect something valuable. Protection requirements are made by controls, and control protects against threats. So, that is how you will have to read it, now in simple terms, you have an information asset, you have an asset value for that. Let us say it is a critical server, which has your programming code inside in the software developed by a team. So, you quantify the value for that I am putting an asset value, then you identify what are all the vulnerabilities that will impact the information asset.

Then identify the threats, which will exploit the vulnerabilities, then the associated risk. So, once you arrive at all this, you know that I need to protect the system, using these many controls, and this is going to be the cost of that. Basically, you get a whole idea of what your control measures are going to be, this process is the risk assessment process, now there is another process called a risk mitigation process.

So, you see the controls here, now the controls here quick fixes we are counter measures all of these will come under your risk mitigation process, are combination of risk assessment, and risk mitigation will give you the risk management process. Now, there is one more thing to note here, what happens if the protection requirements are more than the value of the asset, that something to be thought of right. You transfer the risk to an insurance is transfer of risk right your third party, that is one you rethink about the asset, that is you repair, you replace or retire by putting in a new technology.

(Refer Time Slide: 16:09)



The slide features a dark blue header with the title 'Digital Threats' in yellow. To the right of the title is a small video inset showing a man with a beard and glasses wearing a red and white plaid shirt. Below the header is a white area containing a bulleted list of digital threats. At the bottom of the slide is a dark blue footer bar.

Digital Threats

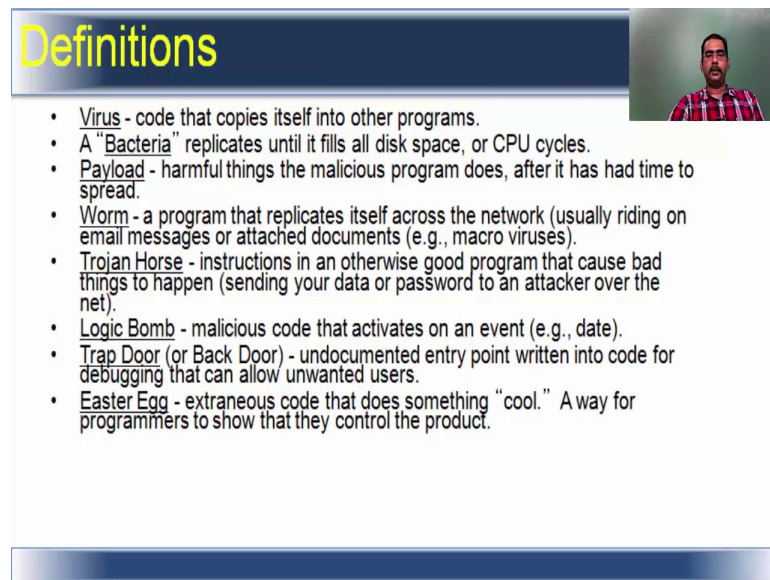
- Viruses, Spyware, Trojans & Other Malicious Software
- Botnets
- Phishing & Spam
- Identity Theft
- Cyber Stalking, Cyber Bullying, Online Predators
- Etc., etc., etc....

So, these are also important factors, to consider let us talk about what the digital threats

are, we will just take a look at viruses, spyware, trojan horses and other malicious software, botnets, phishing, and spam identity theft, cyber stalking, bullying, online predators etc, there are so many terminologies available here, skimming is one. We just not mention here, farming is another one.

So, there are different kinds of digital threats, that are available or that are there. The more the technology improvement, the more the threats, but let us take a look at the basic once, or the once which are been there for a long time.

(Refer Time Slide: 16:58)



Definitions

- **Virus** - code that copies itself into other programs.
- A "**Bacteria**" replicates until it fills all disk space, or CPU cycles.
- **Payload** - harmful things the malicious program does, after it has had time to spread.
- **Worm** - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).
- **Trojan Horse** - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- **Logic Bomb** - malicious code that activates on an event (e.g., date).
- **Trap Door (or Back Door)** - undocumented entry point written into code for debugging that can allow unwanted users.
- **Easter Egg** - extraneous code that does something "cool." A way for programmers to show that they control the product.

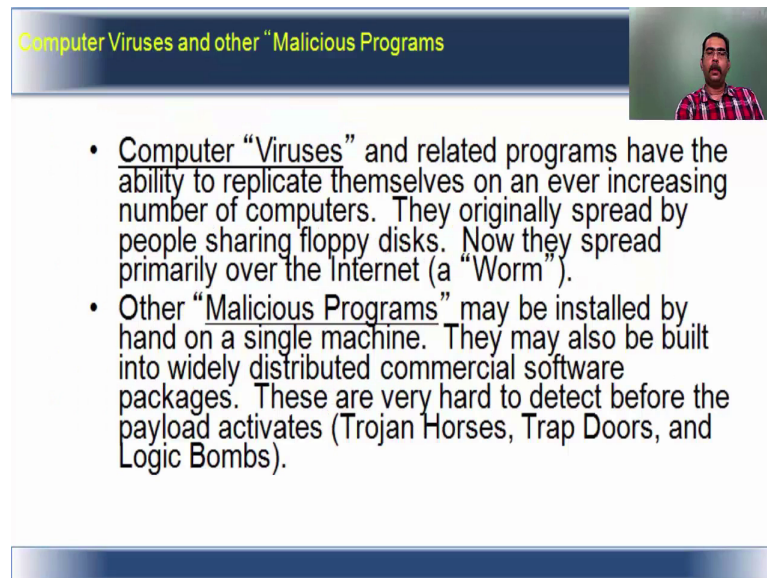
So, that will get a basic understanding of what a digital threat is, let see some definitions. Virus is a code, which copies itself into other program. There is also an expansion for virus which is vital information resources under siege, which is why it is called a virus. So, it is basically a code, which copies itself to other programs. What are the bacteria, bacteria replicates until it fills all disks, or a cpu cycles.

What is a payload, payload is some harmful things, which the malicious program does after it has at time to spread. Worm is something, which replicates itself across the network in generally riding on email messages, or attached documents like macro viruses. Trojan horses are instructions in an otherwise, good program that cause bad things to happen.

We will discuss about Trojan horse also, logic bombs we have already discussed in module one and again in the preceding slides trap door, undocumented entry point written into the code for debugging, that can allow any unwanted users. It is generally

left by programmers. So, that they need not access the front end, and go to the program. So, they just have a trap door or back door, set before they have direct access to the program, then easter egg is an extraneous code that does something cool.

(Refer Time Slide: 18:29)



Computer Viruses and other "Malicious Programs"

- Computer "Viruses" and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a "Worm").
- Other "Malicious Programs" may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).

Will talk about most of this in the subsequent slides, computer viruses have the ability to replicate themselves on an increasing number of computers, they originally spread by people sharing floppy disk. So, in olden days are during the advent of computers, when floppy disks were popular, they used to spread through floppy disks. Now, they primarily spread over the internet.

So, basically a worm spreads over the internet, other malicious programs have been installed, by hand on a single machine. They may also be built into, widely distributed commercial software, they are very hard to detect, before the big payload activates like as Trojan horse, or a trap door, or a logic bomb.