Information security - IV

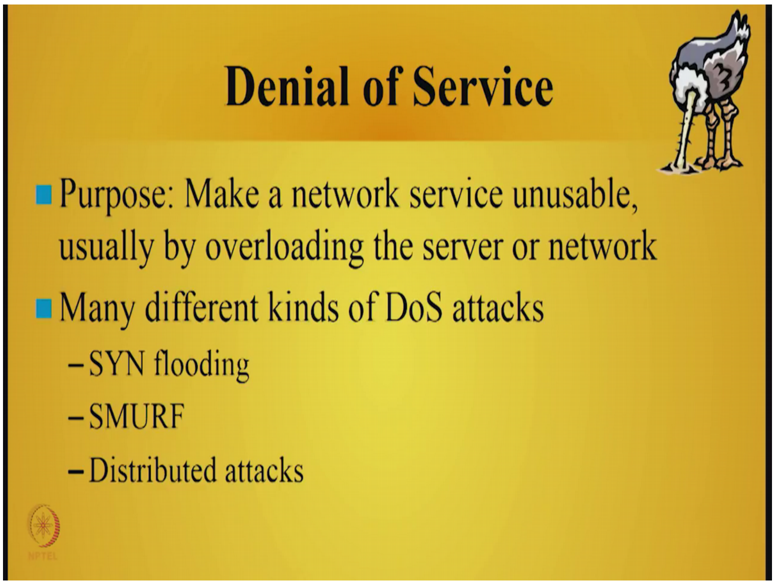
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 11

Network Security and Forensics (Protecting computers connected through the Internet) Part 2

Hey, welcome to this session on network security and forensics. This is a part of the information security fore course..

(Refer Slide Time: 00:21)



Denial of Service

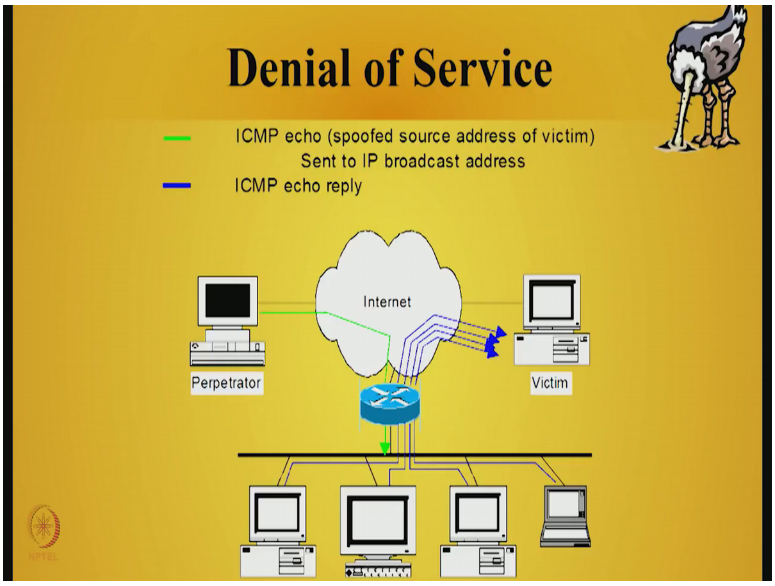
- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks

The third kind of stuff that you can do for example is denial of service. Now, this can be protected using an ideas. So, the idea behind denial of service is that you ensure that your network service is unusable ok. For example, if I have TCP, so it is it is a kind of you have watched it in movies, where someone tries to greet the other person, one person says this, the other person says this and both of them do not converge. So, it is the SYN flooding is similar to that. For example, in TCP protocol you send a SYN packet and then you get a SYN plus ACK and then you are supposed to ACK.

Now, suppose I send a SYN packet and then the other guy sends a SYN plus ACK packet no I do not ack. So, what will happen the other guy will be expecting a response from me. What happens to the other person is that he is expecting an ACK. So, he might be reserving certain kinds of resources and if we do not send him an ACK, he will be keeping those resources for a certain period of time.

Suppose I send lot of SYN packets ok, so since he is keeping the resources for a certain period of time the system might run out of resources; and because of which no other connection for a certain period of time can happen. So, what I will do, what I will do is after a certain period of time, I will stop this attack. Now, after at that time other connections would be accepted. Again after a certain time, so if I do it in random fashion the whole availability will be at risk of the machine. So, this can be detected by intrusion detection systems and we can prevent it.

(Refer Slide Time: 01:48)

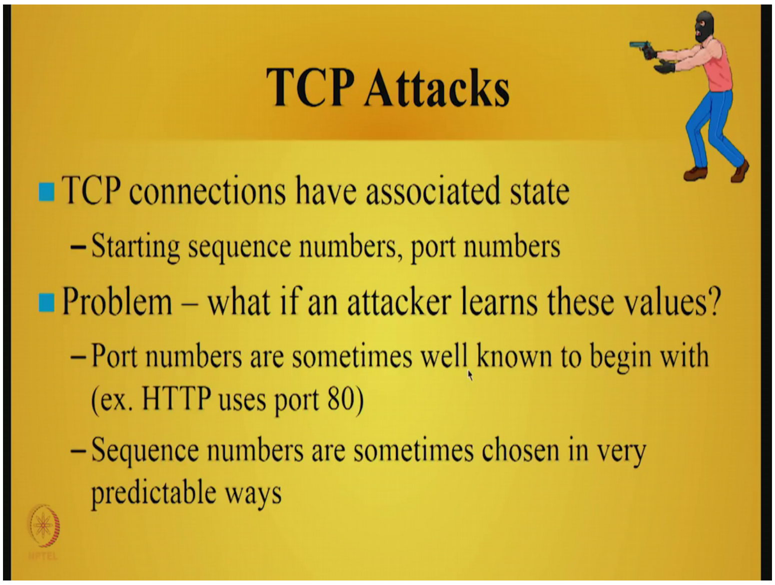


Denial of Service

🟩 ICMP echo (spoofed source address of victim)
Sent to IP broadcast address
🟦 ICMP echo reply

Here is an example of ICMP echo ok. So, here what we actually do is a perpetrator ok. What he does is he makes all the he gets access to all the other missions and the ask them to do a ping ok. So, what will happen is that once I do this every machine will do a ping to this victim, and thereby this guy generating one packet and then making them this can this we can actually make it attack at a certain time also ok. So, what will happen is suddenly this guy will start getting lot of ping packets ok. So, this kind of stuff can be done. You can also spoof source address of a victim; and ensure that he is denied certain kind of service, because this network you know all know that if the network bandwidth is full, you would not be able to download movies or anything, it is just similar to that.

(Refer Slide Time: 02:38)



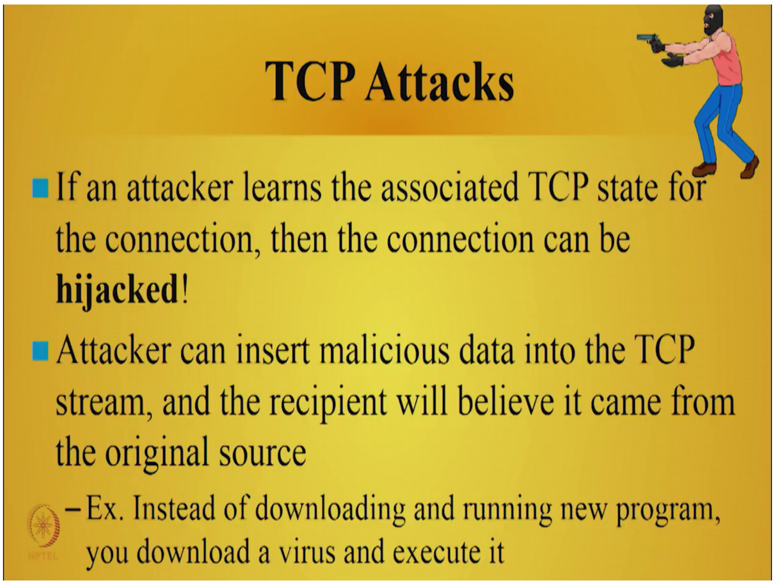
TCP Attacks

- TCP connections have associated state
  - Starting sequence numbers, port numbers
- Problem – what if an attacker learns these values?
  - Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  - Sequence numbers are sometimes chosen in very predictable ways

The other kind of attack that people can do is the t t TCP connections ok. Each TCP connection has an associated state sequence number etcetera. What if an attacker learns these values ok. So, what will I do once I learn these values then I will know for example, TCP HTTP is from port 80. So, what I will know is if port 80 is open, then you know that some kind of a HTTP service is expected on that port. Now, what I can do is I can write a software and then start attacking the port 80 HTTP port 80.

So, then if I come to know that sequence numbers are chosen in some predictable way then I can generate those sequence number and send my own data. So, what will happen is the other person on the other side will start accepting the data my data and totally even if it is a software or anything it will get confused, because it was expecting some other data with this sequence number, but I am sending a different data with the same sequence number. So, all these types of attacks can happen with TCP ok.

(Refer Slide Time: 03:40)

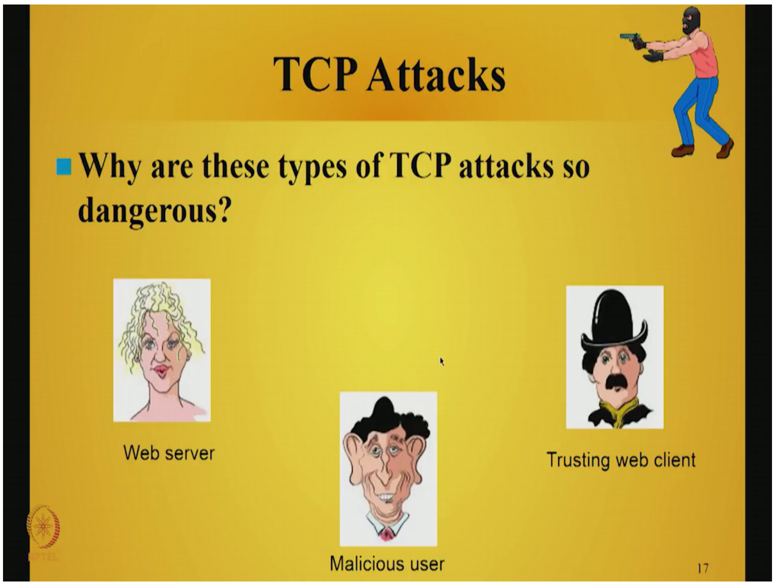


TCP Attacks

- If an attacker learns the associated TCP state for the connection, then the connection can be **hijacked**!
- Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  - Ex. Instead of downloading and running new program, you download a virus and execute it

If I know what is going to be the state of the connection then I will be able to hack that state, and I will be able to hack that connection also. So, in this way the attacker can in insert some kind of a malicious data. And say for example, it is a banking transaction ok, instead of saying 50 rupees, I make it as 5000 rupees ok, and if I can insert this kind of malicious data and I be able to become extremely rich very quickly. So, so, so, so in this way if I can intercept the TCP connection I will be able to do lot of harm to the other person.

(Refer Slide Time: 04:21)

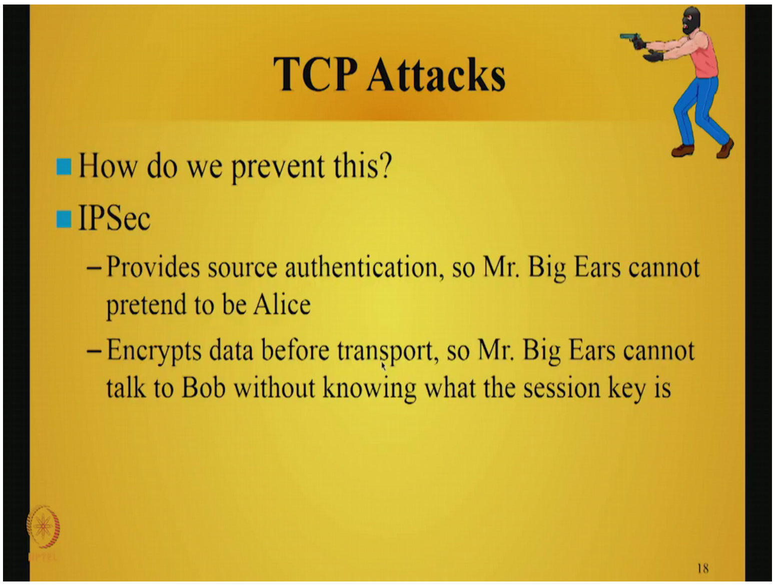


TCP Attacks

- **Why are these types of TCP attacks so dangerous?**

So, this is the wave for example, there is a web server, and then there is a trusting web client, let us assume that instead of directly communicating these two guys directly communicating, someone a malicious user say sits in between. Then this malicious user can actually use drop so he has a bigger here ear, so that you will be able to listen to all the conversations happening between these two types of people that is one type of factor. There are many types of attacks we will see the what are the types of attacks in the future courses. And what we will be concentrating on see the idea behind this sessions are that you need to understand how network forensics can help you detect these kind of attacks.

(Refer Slide Time: 05:03)

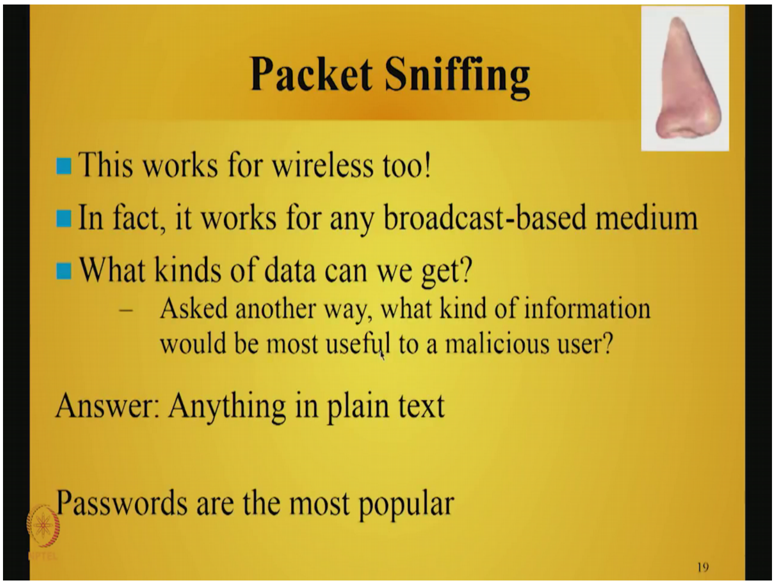


TCP Attacks

- How do we prevent this?
- IPSec
  - Provides source authentication, so Mr. Big Ears cannot pretend to be Alice
  - Encrypts data before transport, so Mr. Big Ears cannot talk to Bob without knowing what the session key is

So, one of the ways you can prevent this kind of eavesdropping from happening is known as IPSec ok. So, this IPSec provides you source authentication ok. So, to ensure that you know that the person to whom you are talking is well known to you ok. And it also encrypts data before transport, so that the person in between cannot present to what the other two people are talking.

(Refer Slide Time: 05:26)



Packet Sniffing

- This works for wireless too!
- In fact, it works for any broadcast-based medium
- What kinds of data can we get?
  - Asked another way, what kind of information would be most useful to a malicious user?

Answer: Anything in plain text

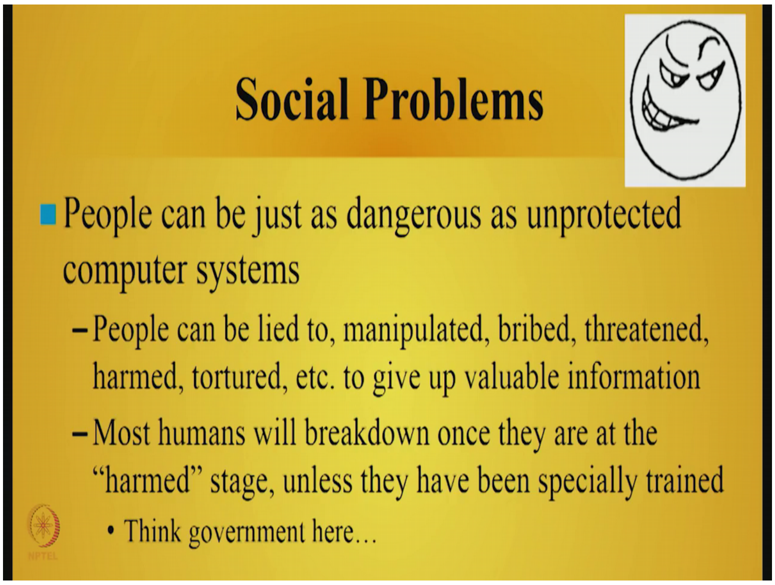
Passwords are the most popular

19

Ah The other type of attack is packet sniffing and. In fact, we will we will be using a tool known as wire shark, and we will be doing a packet sniffing. So, the idea behind packaging is that you want to get what kind of data is going through in my network ok. And sometimes it so happens that some of the email passwords will be sent in plaintext. For example, if you remember the previous diagram that we saw there was this demilitarized zone where there was this email server. Many organizations have their own local email server. And in the local email server they might be actually sending password in plain text ok. Ah

You do not have to worry about Google, because Google uses HTTPS, which is, but if you are not using Google kind of a of a public email client your organizations own client if someone sniffs into the network they might be able to get the passwords ok. Especially many of that SNMP protocols and things like that they actually encode, but those encoding are easy to break. So, passwords are the most popular phrase where people look at and try to find out when they do a packet sniffing attack.

(Refer Slide Time: 06:37)

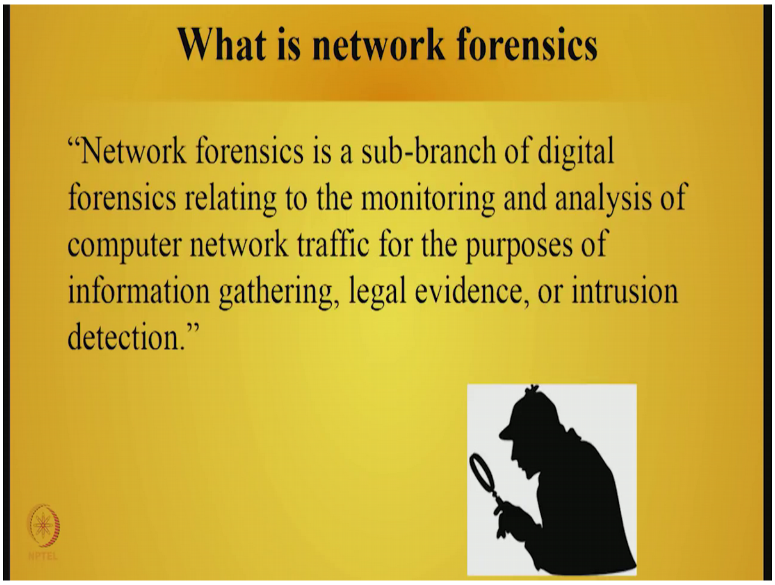


Social Problems

- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  - Most humans will breakdown once they are at the "harmed" stage, unless they have been specially trained
    - Think government here…

And as I told you people can also be as dangerous. So, people can be lied to they can be manipulated, they can be bribed, they can be threatened, harm, torture etcetera. Most of the humans so will break down at a harm stage. For example, I mean you can always going and accepting that my computer is not hacked, but at one point if your personal data goes out, you feel that yes something that has happened here ok. So, anyway, so the social engineering attacks is also very important we will not be covering any of the social engineering attack we will be restricting ourselves to network attacks and network forensics.

(Refer Slide Time: 07:15)



What is network forensics

"Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection."

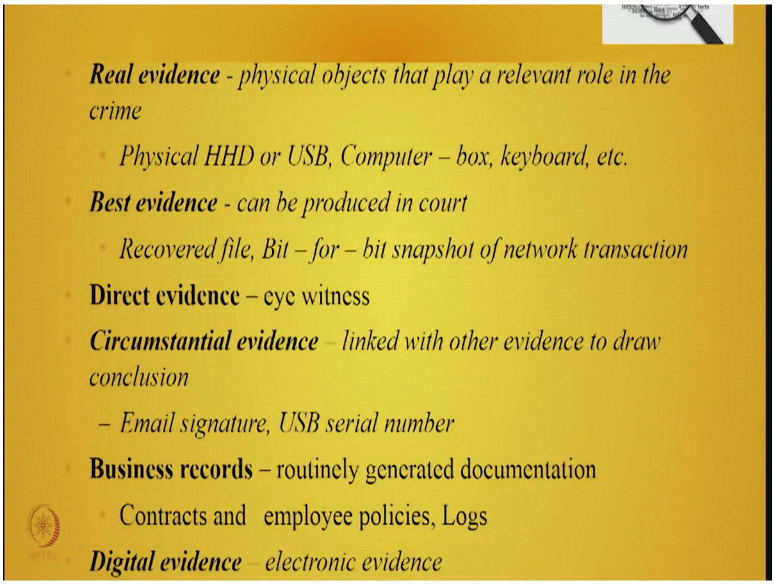
So, the question is what is network forensics? Network forensics is a sub branch of digital forensics relating to monitoring and analysis of computer network traffic for the purpose of information gathering, legal evidence and intuition detection ok. So, if you remember the previous areas, where we are talking about network security the this model say network security is a looking at a secure architecture, how do you connect computer systems and how do you get secure protocols ok; b - how do you prevent attacks from happening by using this secure protocols.

Now let us suppose that an incident has happened someone has hacked into your network then we will have to identify what has gone wrong into the and why our security mechanisms were breached. Because once the breach happens, then it can lead to data loss. As we have seen data loss can lead to monetary losses, therefore, it is necessary that we identify what is the breach and how do we ensure that this kind of breach never happens. So, the area which helps you to identify what is the breach, how it has happened is network forensic. Once I identify that something has happened first part and this is I have to gather all the information on how an attack has happened. The second part is that I have to give a legal evidence in the court of law ok.

Because any thief who does an abnormal activity denies having done that activity; and it is true everywhere in a legal system ok. So, therefore, it is the burden of the person accusing to prove that something bad has happened. And for that you need legal evidence therefore, you have to collect the data carefully, you can store it carefully, you have to transport it carefully to ensure that there is no leak in the data that you collect or someone does not manipulate with your authentic data that you collect out of this information gathering activities.

And finally, your legal evidence has to show that there is some kind of harm that has happened some kind of intrusion that has happened into the network. So, your intrusion network forensics includes all the three branches, all the three activities information gathering, legal evidence and intrusion detection. So, you collect data traffic computer network traffic to ensure that if a person has hacked into a network, he is legally punished for his wrong doing.

(Refer Slide Time: 09:43)



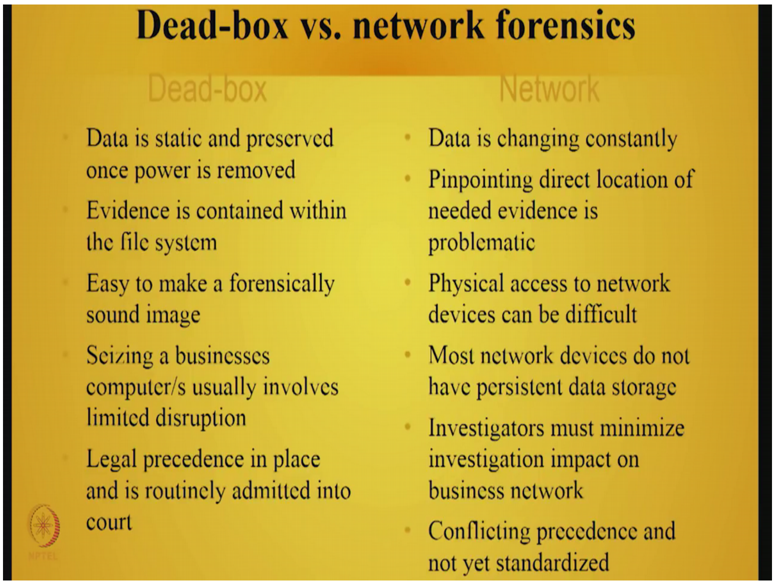
- ***Real evidence*** *- physical objects that play a relevant role in the crime*
  - *Physical HHD or USB, Computer – box, keyboard, etc.*
- ***Best evidence*** *- can be produced in court*
  - *Recovered file, Bit – for – bit snapshot of network transaction*
- **Direct evidence** – eye witness
- ***Circumstantial evidence*** *– linked with other evidence to draw conclusion*
  - *– Email signature, USB serial number*
- **Business records** – routinely generated documentation
  - Contracts and employee policies, Logs
- ***Digital evidence*** *– electronic evidence*

The first thing that we should understand is what is in evidence ok. There are different types of evidences that one can come across. One is the first one is the real evidence, where you have physical objects that play a relevant role in the crime ok. For example, yeah USB drive that was inserted or yeah physical hard disk drive that you can produce in the court of law. So, these are all real evidence. For example, I had stored a malicious software or a transferred data for which I have no access, I should not be having access I have that data in my hard disk. So, in that case what I can do is I can bring my hard disk and then show that yes this data was not supposed to have been accessed by me, but it is there in my hard disk.

The second evidence is the best evidence that can be produced in court for example, a file that was recovered or email that was required and bit by bit trans snap shot of some network transactions that had happened etcetera. The third one is the direct evidence where an eye witness can come and say that yes I saw this guy typing the password and doing these kind of illegal activities etcetera. The forth is known as circumstantial evidence ok. So, these are evidences that are linked with other evidence to draw a conclusion. For example, an email signature ok. So, if I had sent an email with my signature then it means that it I have originated the data ok. So, next is the now it is email signature, for example, if its entered digital signature then it becomes one of the direct or the best evidence ok. But if you had sent just an email signature writing my name then can only be considered as something that is circumstantial because I could always claim in the court of law that someone had typed my name there ok.

The next one is the business records it is the logs or the routinely generated documentation, contracts etcetera ok. And finally, you have the digital evidence which is an electronic evidence such as signed emails ok, signed documents, log files that we get out of intrusion, detection, prevention firewalls or operating system etcetera. So, these are all the different types of evidences that one can come across.

(Refer Slide Time: 12:02)



Dead-box vs. network forensics

Dead-box

- Data is static and preserved once power is removed
- Evidence is contained within the file system
- Easy to make a forensically sound image
- Seizing a businesses computer/s usually involves limited disruption
- Legal precedence in place and is routinely admitted into court

Network

- Data is changing constantly
- Pinpointing direct location of needed evidence is problematic
- Physical access to network devices can be difficult
- Most network devices do not have persistent data storage
- Investigators must minimize investigation impact on business network
- Conflicting precedence and not yet standardized

Now, there is a difference between network forensics and something known as a dead box ok. In your dead box, for example, I just want to find out what is there in a hard disk that is a kind of a dead box ok. For example, a data is static and preserved once power is removed it is for example, a hard disk is a kind of a dead box where the data is static and once the power is removed the data still exists there. And evidence is contained in the form of a file system ok.

So, the advantage of having a dead box is that since you have the data that is available to you, you will be able to forensically analyze it and then get a sound image of what had happened. The other thing is there is not much of a disruption of business, because once I find there are some digital evidences, I just take away just this disk or something or a USB or whatever it is and then what I do is I can give them another disk where they can continue working ok. And this kind of dead box that is always legal presidents in place ok, it is like keeping a kind of files ok, the normal paper files for producing evidence.

The network forensics what happens in the network is the data is always changing constantly I mean you can see that the internet lot of data gets transferred and this packets get intermingled in the internet. And in order to determine a flow, you just have to trace the packets of a particular ID, so that you get a kind of a flow. Whereas, if you take a dead box like let us say a hardware drive a hard disk drive, now set of a file that is related can also be traced something by using the super block or a block chain etcetera, I am not talking about the block chain that we used in security aspect. I am talking about the chain of blocks.

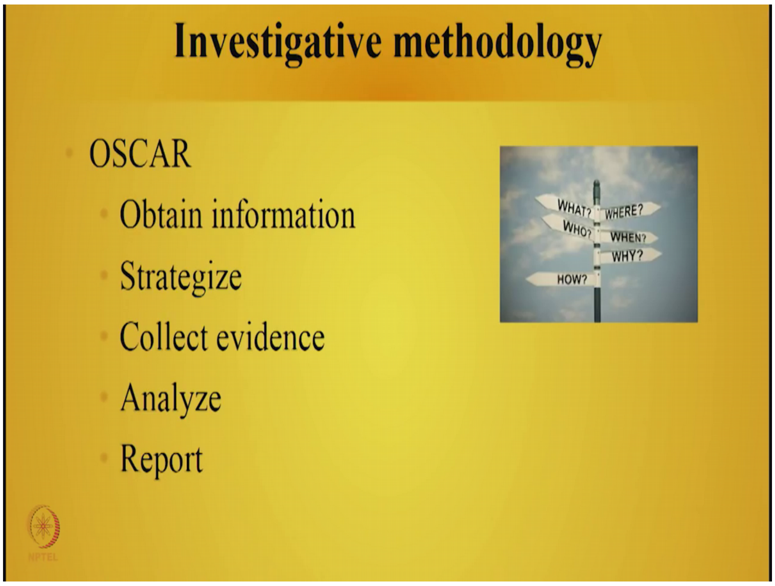
Now, pinpointing direct location is of needed evidences problematic one of the things that could happen with network forensics is that the timelines could lie in different time zones ok. For example, the data could have travelled from US to UK to Europe and then back to India ok. Now, look at there are about seven or seven or eight time zones that are involved when this data gets transferred. So, even if someone had mistakenly configured sometimes or wrongly people might say that it is not an acceptable evidence so that is the next problem. Whereas, in your hard disk many of many a time the files actually get stored along with the date and time stamp.

The third one physical access to network devices can be difficult because network devices are owned by private companies ok, in my internet service providers. And they might not an a law that is applicable in India may not be applicable abroad ok. So, you might have to have some kind of see we were seen that in many of the many of the crimes that happened people go abroad and to bring them back to India it becomes extremely difficult, because of the lot of legalities that are involved. You have to prove that that person has done a crime and then he has proved that he has gone out of and those quotes may not accept etcetera. Now, such problems can exist in terms of network also ok.

The other point is that well we are collecting now logs from network devices, but how long will these network devices store the logs, because if you remember the routers links have huge bandwidths and storing all the data at that bandwidth will require enormous storage area. And the network devices does not have that much of storage area have very limited storage area. So, can you store all the logs usually they recycle the logs, and they might have logs for 24 hours or 1 week etcetera. And, so you might have to take the data out of those boxes as quickly as possible ok; whereas, this may not be the case with a hard disk drive evidence that you have at hand.

The other aspect is that investigators must minimize investigation impact on the business network because I cannot be injecting lot of packets and wasting the bandwidth of the company while trying to do an investigation ok. It is like you stamp over all the place of a crime scene and then you find it difficult to identity who was done the crime ok. And today at least there is conflicting precedence over what data to collect and then all these things have not been standardized anyway.

(Refer Slide Time: 16:36)



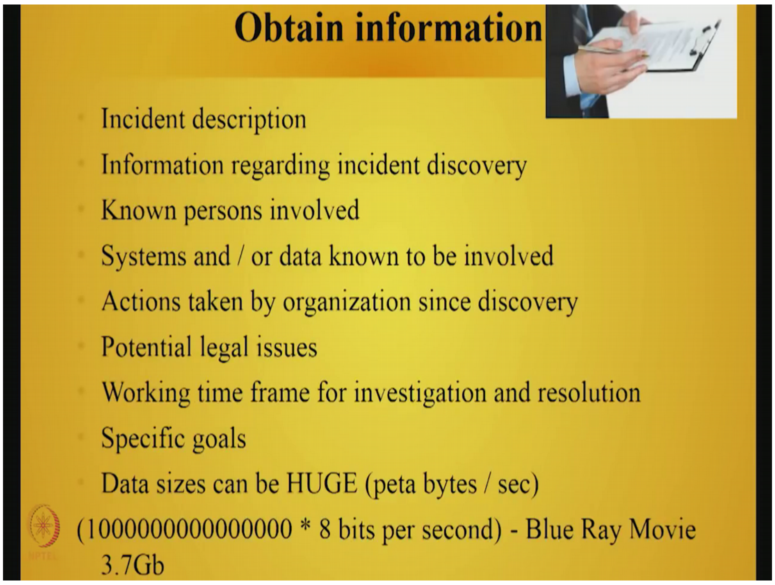
Investigative methodology

- OSCAR
  - Obtain information
  - Strategize
  - Collect evidence
  - Analyze
  - Report

WHAT?
WHERE?
WHO?
WHEN?
WHY?
HOW?

Usually the investigative strategy is called OSCAR, but there are five stages. One is you obtain information ok, two you strategies, and three you collect evidence, four you analyze and then five you report. Now, all these things you do, so that it forms a legal evidence; that means, not even at one point it should so happen that there is a leak where I say for example, either obtaining the information and strategizing it everything should be authentic.

(Refer Slide Time: 17:09)



Obtain information

- Incident description
- Information regarding incident discovery
- Known persons involved
- Systems and / or data known to be involved
- Actions taken by organization since discovery
- Potential legal issues
- Working time frame for investigation and resolution
- Specific goals
- Data sizes can be HUGE (peta bytes / sec)

(1000000000000000 * 8 bits per second) - Blue Ray Movie 3.7Gb

So, what is obtaining the information? So, what you should do is you should have a brief description about the incident, what has happened, how the hack has happened etcetera. And how someone discovered that such an incident has happened. Whether known persons were involved in the incident, whether the system under data or known data known to be in one, see whether you know whether what are the data that has been lost ok, what are the systems that have been compromised etcetera.

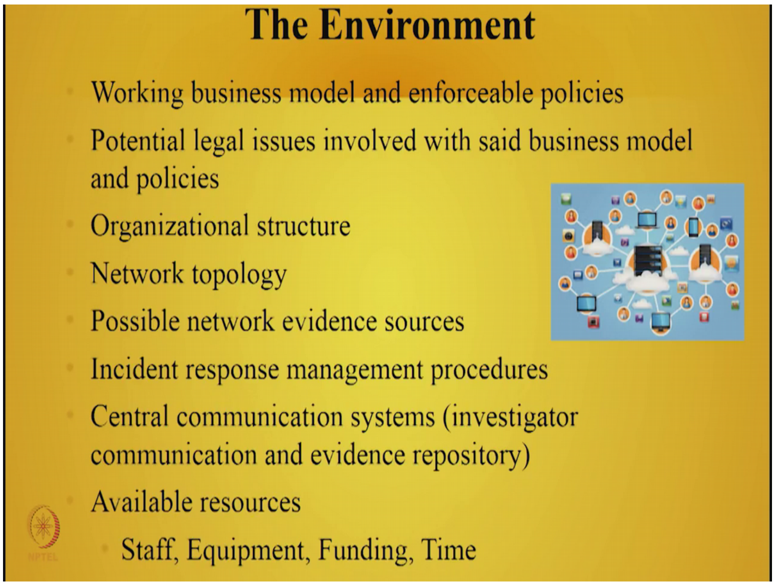
You should also obtain information about what the organization has done since the discovery of a data breach ok. So, whether they have remote access to the network or we have only disconnect to the network or the company shut down the whole network etcetera, then they should also study the impact of the potential legal issues. If a data of a lot of subscribers have been compromised, then it could lead to lot of litigations, therefore, you should look at potential legal issues that has occurred due to the breach of data ok.

And you should also look at working time frame for investigation and resolution. You should say approximately you would be able to do this kind of work in this amount of time. You should also find out one of the specific goals of your investigation I mean you just cannot be beating around the bush. One of the things you should take into account is that the data sizes can be huge ok, so for example, I blue if you a blue ray movie is around 3.7 GB, but if you look at router that transfers beta bytes per second of data, now

I have given you the numbers ok. So, you have to multiply that is 8 followed by so many zeroes and that is per second. So, you need to you can find out how many bits of data can be is need to be stored to obtain the information.

The second one is the environment ok. So, you should also study the organizations policies ok. What is the business model of the organization, what is the organization structure, what is the network topology that the organization is used ok, and what are all the possible network based evidences that you can get. Similar, remember I mean you should also look at camera based evidences, because if someone steals a data and puts it in a USB drive and takes it home how will you prove it. I mean you have to show that the person has entered that place, he is removed the USB drive and then he has taken into a home etcetera.

(Refer Slide Time: 19:28)

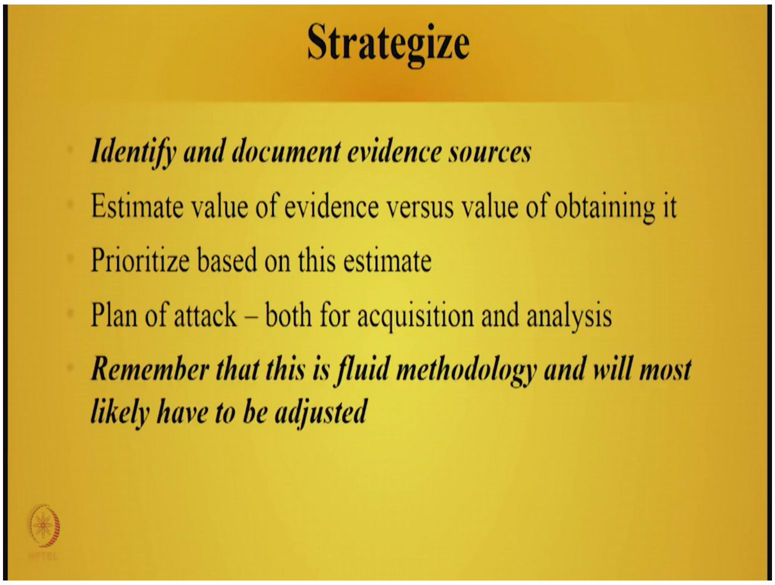


The Environment

- Working business model and enforceable policies
- Potential legal issues involved with said business model and policies
- Organizational structure
- Network topology
- Possible network evidence sources
- Incident response management procedures
- Central communication systems (investigator communication and evidence repository)
- Available resources
    - Staff, Equipment, Funding, Time

Then you should also look at the incident response management procedures, we should also look at available resources for I mean at the time of the incident and for the investigation etcetera.

(Refer Slide Time: 19:40)



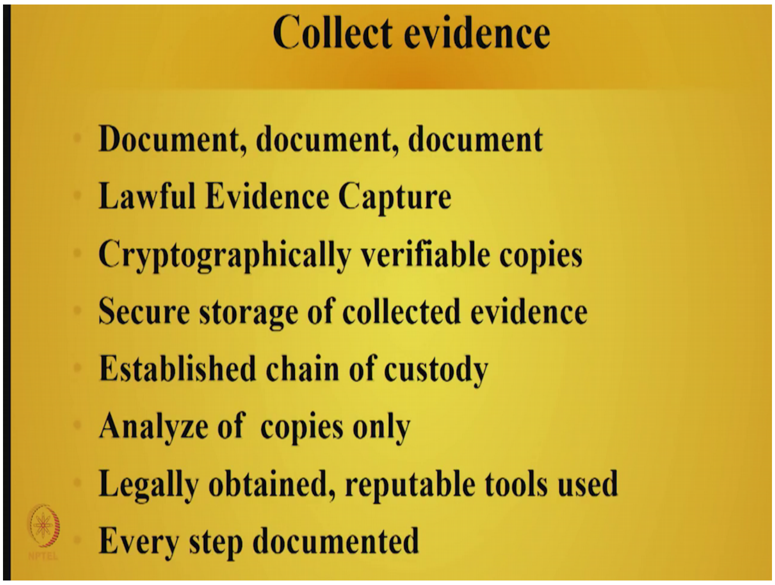
Strategize

- ***Identify and document evidence sources***
- Estimate value of evidence versus value of obtaining it
- Prioritize based on this estimate
- Plan of attack – both for acquisition and analysis
- ***Remember that this is fluid methodology and will most likely have to be adjusted***

The third one is strategizing the whole thing ok. You first have to identify in document evidence sources and these evidences have to be preserved very carefully. There are many incidences where the investigating agencies have collected the data they kept it in the c d drive ok, but when they come and show that in the court of the law nothing comes out of the CD drive ok. So, it for magnet tapes, for example, when you are carrying the magnetic tape in your hand, someone just puts a huge magnet in his pocket and walks by that tape anything can happen you know so these are some mechanisms I will it be will people will try to tamper the evidences.

The second one that you need to do is estimate the value of these evidence versus the value of obtaining it ok. So, the value of the evidence is high then you have to spend lot of time to obtain the evidence I mean usually; that means, the value of time that you spend could be high. But if the value of evidence is very low, then do not spend a lot of time to get that evidence. And you should actually once you get the estimate of the value of the evidence then you priority is based on this estimate like these are all the evidences that I must collect there is a set of evidences that I may collect and set of evidences that are good to have. So, you should also look at how you are going to acquire data and how are going to do the analysis ok. And you need not be very stringent any of this methodologies you should be very flexible enough, but not too flexible I mean these are all very generic terms, but you will come to know of it once we do some kind of case studies.

(Refer Slide Time: 21:22)



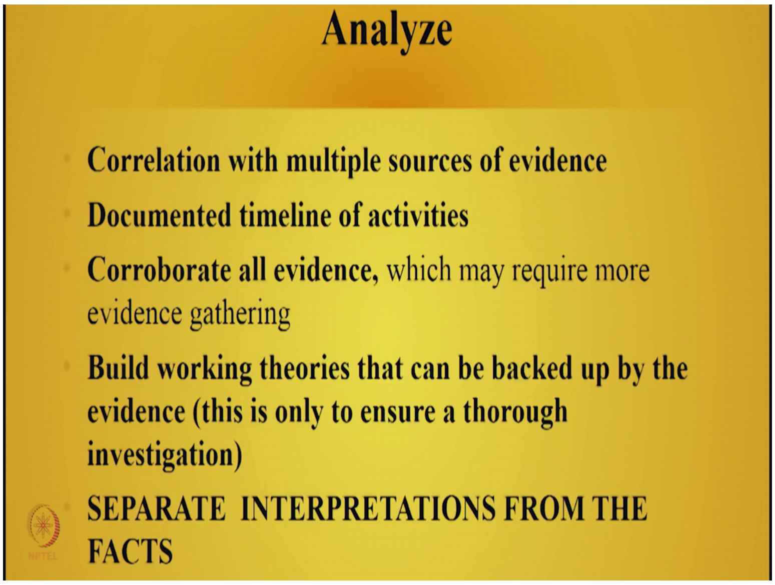
Collect evidence

- Document, document, document
- Lawful Evidence Capture
- Cryptographically verifiable copies
- Secure storage of collected evidence
- Established chain of custody
- Analyze of copies only
- Legally obtained, reputable tools used
- Every step documented

The next one is collecting the evidence and one of the most important thing is document, document, document, whatever evidence you collect it has to be documented. The second thing that you have to do is as much as possible you have to do a lawful evidence capture ok. For example, one of the things that people do now is to find out whether the government does precede certain orders put an RTI. So, RTI is usually accepted as one of the legal evidence. The third one is you should also have cryptographically verify verifiable copies of the evidences. And the evidences must be stored securely. The other most important part with evidence is see you should not trust anyone while handling evidence, because any human being can be compromised by social engineering strategies. Therefore, even if a evidence is handed over from one person to another person that is the chain of custody has to be established ok, so that you can find out who exactly could have done something wrong while handing over the evidence.

The next one you should look at is you should always analyze copies of evidences. Never use the original evidence to do some kind of analysis. Make a copy of the original analysis and do the analysis, because if the original evidence is lost your old case is lost. You should also use legal tools and reputable tools. Reputable reputation comes out of the tools performing well in case of getting in the evidence. So, I would not train you much stress on reputable tools, but at least you should those tools should be legal. And please document every step of the work that you do. Finally, you have to do an analysis of the data that you have got ok.

(Refer Slide Time: 22:58)



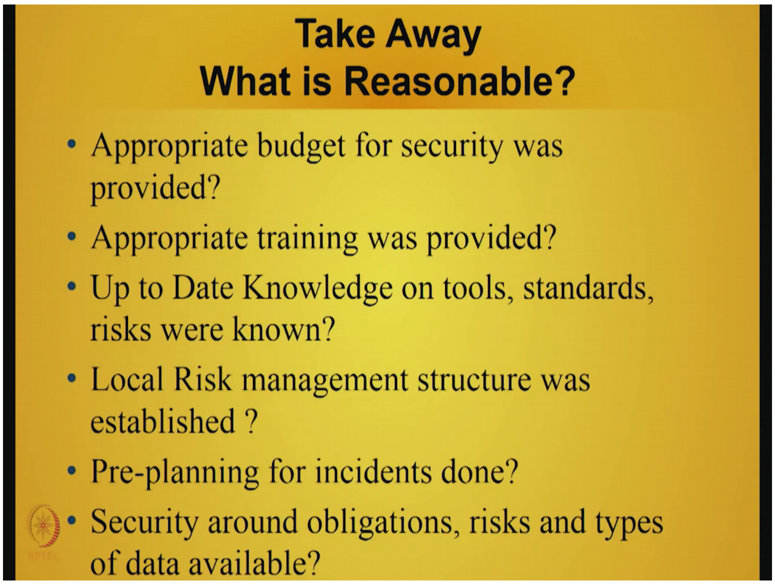
Analyze

- Correlation with multiple sources of evidence
- Documented timeline of activities
- Corroborate all evidence, which may require more evidence gathering
- Build working theories that can be backed up by the evidence (this is only to ensure a thorough investigation)
- SEPARATE INTERPRETATIONS FROM THE FACTS

First foremost is separate interpretations from facts ok. It is told in Sherlock Holmes that when that (Refer Time: 23:07) asked how is able to detect all these clues, he said if I remove whatever is not possible then what remains as impossible is the possibility. So, in that way, so you would separate interpretations from your fact ok. So, you find out what the facts are and get interpretations out of the facts and not your own interpretations and think that the fact will be there for my interpretation.

One of the most important things for analysis is correlation ok. You have to correlate multiple sources of evidence ok. Just do not go with one evidence and say yes I have found out what the problem is. Then you should have a documented time line of activities. Now, we will do some case studies we will see some case studies where we will see the importance of all this because all these are kind of soft skill ok. So, for example, corroborating all evidences how do you radiate use kind of some kind of intuition as well as your skills to find how to corroborate these evidences ok. So, and then build working theories that can be bogged up by the evidences, so like do not interpret something ok. So, if you believe that this theory is workable, yes, then look at it as a fact and then look at the evidences.

(Refer Slide Time: 24:21)



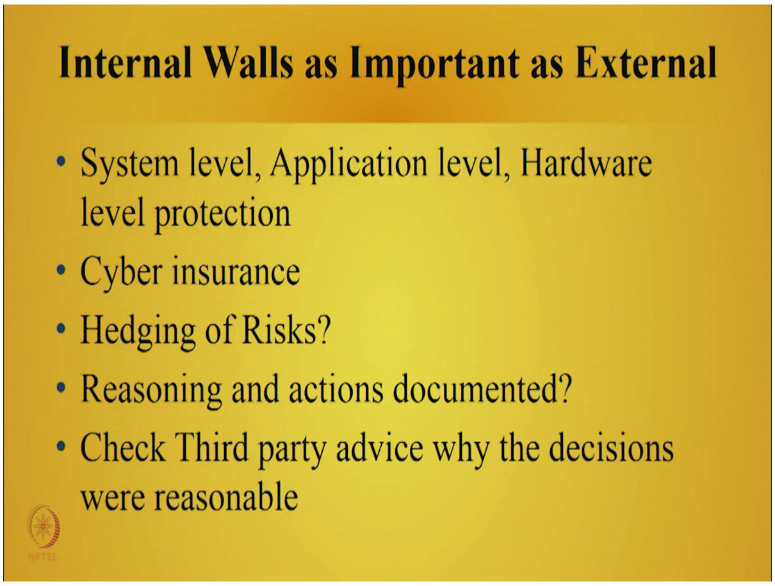
Take Away
What is Reasonable?

- Appropriate budget for security was provided?
- Appropriate training was provided?
- Up to Date Knowledge on tools, standards, risks were known?
- Local Risk management structure was established ?
- Pre-planning for incidents done?
- Security around obligations, risks and types of data available?

What is reasonable ok? So, one of the things that we said was we said about documentation, we said how the organization has prepared itself ok. Some of the questions that you might ask the organization while doing the documentation is first question is have you provided appropriate budget for security ok? Because usually security takes a backseat, see when this there was this problem with year 2000 Y2K problem in which many of these IT engineers were involved the impact that Y2K problem had was very low. So, some people started questioning should we have spent so much money to overcome this Y2K problem I mean when you are very secure you will start questioning whether that much money was needed to provide a security, but even if there is one failure of security we will say that this budget was not enough. So, you need to be very careful security will cost you something. So, you have to find out whether appropriate has been budget has been provided by the organization for security.

After the budget, second one is the training even though you might have lot of budget you might try to buy a lot of tools, but if the people do not know how to use those tools then your security infrastructure is going to be a problem ok. The third one is do you have up to date knowledge on the tool standards under does your organization provide these things. Now, fourth one is give some an impact happens how do you manage the risk. So, where you prepared for the preplanning of say for example, if it is a bank then you need to ensure that the transactions happen securely. Then you should also look at the type of risks, then what is the obligation for example, suppose a data breach has happened, what is the obligation of the organization to the people who are affected by database. Do you tell them immediately or and if you tell them immediately, what type of message do you tell them etcetera.

(Refer Slide Time: 26:18)



Internal Walls as Important as External

- System level, Application level, Hardware level protection
- Cyber insurance
- Hedging of Risks?
- Reasoning and actions documented?
- Check Third party advice why the decisions were reasonable

So, there are lot of other things that you need to look at ok, internal walls within the organization is as important as an external wall. So, for example, what is the system level, application level and hardware level protection, you are going to provide in your systems ok. The previous considerations were a kind of a soft skill kind of consideration. The current control situation like internal walls etcetera like system level, application level, hardware level protection is a kind of infrastructure kind of a protection ok.

Then do you have cyber insurance ok? How will you hedge these risks ok? And reasoning and actions on how you are they document it ok? So, something that has happened how will you document all those things. Then, you should also involve some kind of a third party audit and it is similar to the ISO audits you should also have a security audit of your organization about all these hardware software application level protection etcetera. So, in this way what you could do is that overall when in the area of network forensics it is not only analyzing what has happened, it is also devising prevention mechanisms doing audits all these things put together will give you a very secure framework in which you can operate.

Does it guarantee that no hacks will happen? No, because there is always hackers always use new techniques new algorithms to hack your network ok. Therefore, it is like keeping abreast with all the latest items that are there what are all the things that are happening. And then improving your local network based on the learning of other organization also. With this we complete our introduction on about this course a detailed introduction. And from now on in the from the next module onwards, we will look at how to provide security or how to break the how hackers can break your operating systems and other network devices.

Thank you very much.