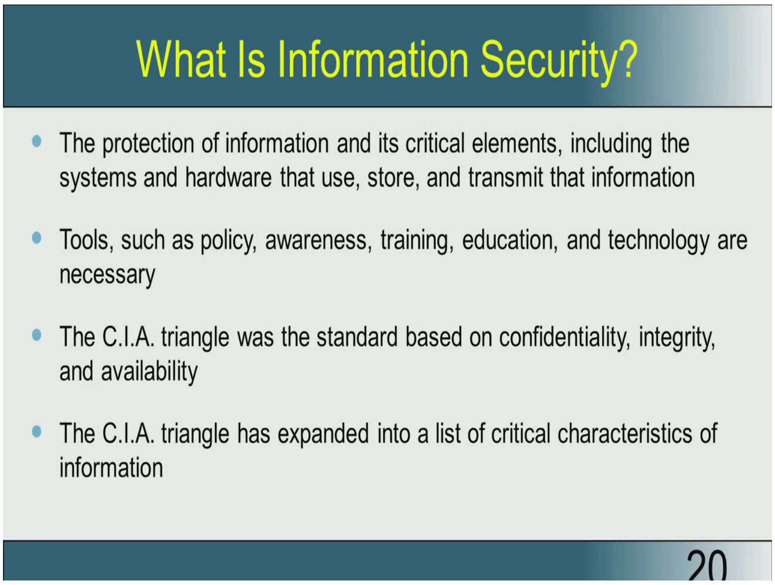
Introduction to Information Security

Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 04

Now that we understood something about security, we also understood something about information, let us now go and define, what is Information Security, the word put together.

(Refer Slide Time: 00:09)



What Is Information Security?

- The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information
- Tools, such as policy, awareness, training, education, and technology are necessary
- The C.I.A. triangle was the standard based on confidentiality, integrity, and availability
- The C.I.A. triangle has expanded into a list of critical characteristics of information

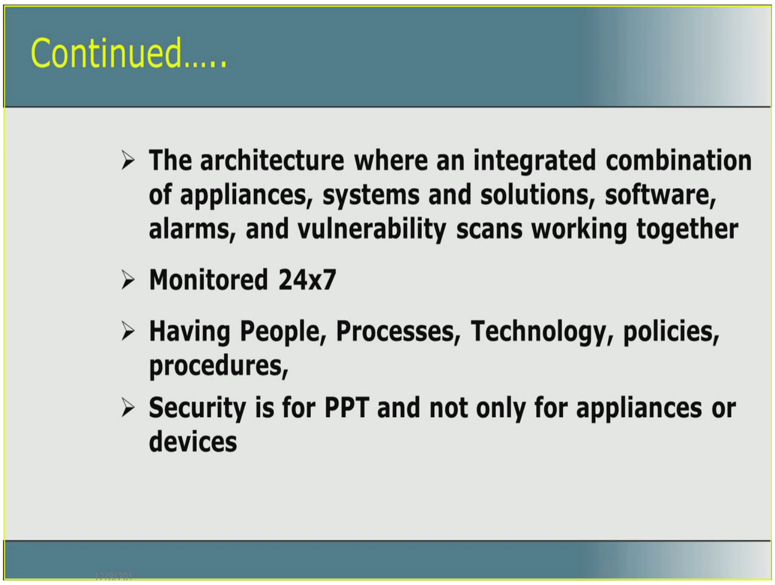
20

Actually Information security is an architecture, now let us go through some definition. Information security is to protect information and it is critical elements including the system, hardware that use, store and transmit that information. So, how do you protect these information, we use tools, what are those tools, tools are not just software. The policy of an organization of how to use the information itself is a tool, the awareness of the different stake holders who use that information is also a tool,

the training you impart on using this information in a secure fashion, itself is a tool. The basic education of the different people is also a tool, the technology that we use is a tool. So, tool for protecting the information need not necessarily be a software or a hardware or a system, but it can be also a policy, it can be a document, it can be the basic awareness of the people, it could be the processes that are followed, all these are tools.

Now, these tools are basically arrived at or the basically designed using the CIA triangle which is nothing but, confidentiality, integrity and availability. The CIA actually forms the basis of security, so the CIA dictates, so every document, every tool that we designed, every document we prepared, every training that we impart, every technology that we procured from for information security purpose is basically associated with some property of the CIA which makes you buy that or which makes you design that.

(Refer Slide Time: 02:30)



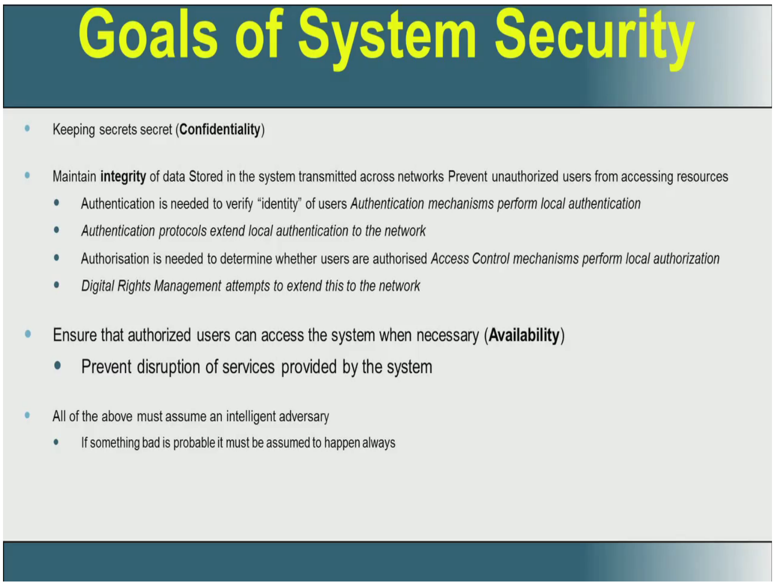
Continued.....

- The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans working together
- Monitored 24x7
- Having People, Processes, Technology, policies, procedures,
- Security is for PPT and not only for appliances or devices

Now, let us go... So, the Information security as you have perceived in the previous slide is nothing but an architecture. What is an architecture? Architecture is actually an integrated combination of several things that makes an architecture. Now, in the case of information security it is an architecture which is an integrated combination of appliances, systems, solutions, software, alarms and vulnerability scans all of them working together and it is monitored 24 cross 7, but it doesn't stop there. The architecture also includes people, processes, technologies, policies and procedures.

So, the security that we are talking of is just not implied only for the appliances or the hardware and the software, it is also applied for the people, the processes that are followed and the technology. So, to sum up we understood what is information, we had some notion of what is information, what is security. Now, we merge these two terms and called it is information security and now we have a sort of a reasonable definition for information security.

(Refer Slide Time: 03:57)



Goals of System Security

- Keeping secrets secret (**Confidentiality**)
- Maintain **integrity** of data Stored in the system transmitted across networks Prevent unauthorized users from accessing resources
  - Authentication is needed to verify "identity" of users *Authentication mechanisms perform local authentication*
  - *Authentication protocols extend local authentication to the network*
  - Authorisation is needed to determine whether users are authorised *Access Control mechanisms perform local authorization*
  - *Digital Rights Management attempts to extend this to the network*
- Ensure that authorized users can access the system when necessary (**Availability**)
  - Prevent disruption of services provided by the system
- All of the above must assume an intelligent adversary
  - If something bad is probable it must be assumed to happen always

Now, let us go forward and talk a bit more on this, now what are the goals of information security. We have just seen it is CIA, Confidentiality, Integrity and Availability. Now, let us go and define these goals. What is confidentiality, keeping secrets secret. I have a secret and I want to maintain, I want to store it in a place where it will we kept as a secret. What is integrity? We have already seen that the data, the way it is stored, the way it is transmitted, dictates what is integrity.

So, integrity itself now gives us more processes that need to be followed for us to go and certify OK that integrity is being satisfied here. So, at least there are two important steps here, authentication and authorization. So, identification, authentication and authorization, there are three steps involved in maintaining the integrity of data. First, somebody wants to use the data, who is that person that is the identity.

So, when you login to your mail server what is the data? The mails are the data and the mails that you want to access, the mails that have come for you alone should be shown to you and that is the integrity. And nobody should see that data, nobody should have manipulated , nobody should have deleted that mail, nobody should have logged in and send a mail on your behalf, so these are all integrity issues.

Now, how do we first identify yourself, we use a user name and that identifies, then there is an authentication. How does a mail server authenticate, you use the password. The moment this authentication happens, then in the mail server there will be n number of mail boxes. For example, Gmail will have millions of mail boxes, you are not authorized, you are been identified by your user name, you have been authorized, you have been authenticated to enter the system by the password, after that now you are authorized to go and touch only your mail box, you cannot go and access anybodies mail box.

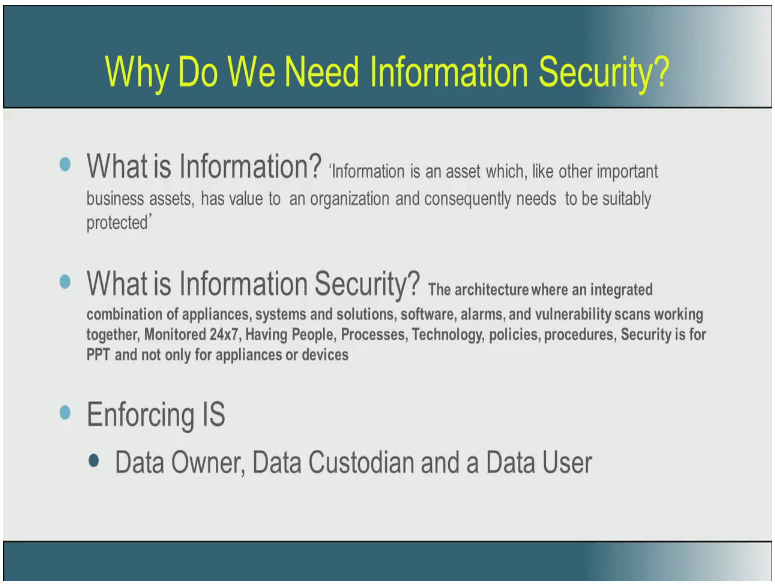
So, there are very simple understanding of what means to have an integrity on the data stored, you need to have these three processes namely identification, authentication and authorization. So, the digital rights management is what; this is a very, very simple way by which one can explain you the digital rights management. I have there is a digital data which is my email and I have a right on that particular digital data.

Different people have different rights on different parts of the data and the management of these rights by assigning which user is authorized to use which part of the data comprises digital rights management and this is a simple way of doing this. Now, we talk of availability. Availability is when an authorized user needs data it should be made available. So, what does it mean that there should be no disruptions to the service provided by the system.

Because, if I don't get the data at some point of time, if the data is very crucial for me and I do not get the data then, the system is not so secure. So, confidentiality, integrity and availability these are all simple definitions of this CIA and all of these above, we should try and maintain confidentiality, we should try and maintain integrity, we should try and maintain availability in the presence of a very intelligent adversary and that should be our assumption, we should prepare ourself for the worst.

So, when somebody designs a secure system, one of the important things, one of the important line that he or she should keep in mind is if something bad is probable it must be assumed to happen always. This sort of an attitude should be developed when somebody conceives of a secure system, somebody tries to make a tool for the secure system, when somebody tries to make a policy for the secure system, this information security makes this very paranoidical sounds paranoid, but this is a truth that you make this assumption, if something bad is probable then it must be assumed to happen always.

(Refer Slide Time: 09:19)



Why Do We Need Information Security?

- What is Information? ‘Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected’
- What is Information Security? The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans working together, Monitored 24x7, Having People, Processes, Technology, policies, procedures, Security is for PPT and not only for appliances or devices
- Enforcing IS
  - Data Owner, Data Custodian and a Data User

So, why do we need this information security, we have understood what is information, we have also understood what is information security. Now, we should talk of before going to understand why do we need information security, now we should talk of people who are going to enforce this information security. Now, information is basically data, when it is processed it becomes information. Now, for this data there is a owner, there is a custodian and there is a user.

For example, if you take a bank, the management the board of the bank is the, the management of that bank is the owner of the, say the core banking. The custodian is the system integrator who actually manages this data along with a part of the information technology team of the bank. And the user is the employees who manipulate this data, who works with this data and also the customers who also use this data and who goes and changes these data through the internet banking and alternate channels.

So, there are three people involved when you look at data, who owns the data, who is the custodian of the data and who uses this data and these three are very distinct. The data owner is the person who is responsible to say who can use this data, who is authorized to touch which part of the data, what is the hierarchy, what is the access rights essentially the digital rights management is enforced by the owner. Then, there is a custodian to whom these principles are told, it is entire policy is told. So, the data owner makes the policy and these policies are told to the custodians.

The custodians implement these policies and prove to the data owner that these policies are indeed implemented, the data owners conduct audit to find out whether the policies that they have stated are indeed implemented or not. The custodians also look at regular backups, why backups are important, why are we talking about backups here, because availability is an issue there. The custodians also look at integrity, so they put they are responsible for designing hardware and software such that the data is stored in the integral fashion.

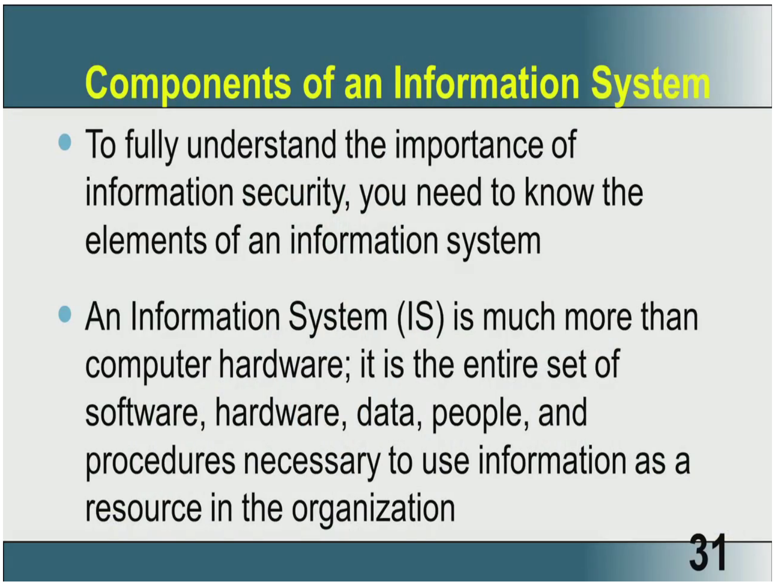
The integrity of data is ensured by the custodian and of course, the confidentiality of the data is also ensured by the custodian by making provisions for hardware and software which can get us this confidentiality. For example, we use a trusted network to transmit data, we use at encryption to store the data, these are all ways by which I go and get confidentiality, integrity and availability. Of course, the data user are the users who use this data and there is also a security associated with the user.

For example, to a bank customer we have given password on the internet. He is not supposed to announce that password, he is not supposed to right that password, we have start for the information in some of the previous slides there were at least 20 different things one can do with the information and all those things that a user can do with a password, you should do it with some discipline and if that discipline is not followed, then there is going to be a vulnerability.

So, ultimately it is the people who are going to enforce these information security policies and they are going to be the data owners, they are going to be the data custodians and they are the data users and everybody has a responsibility in bringing up, in ensuring information security in a system. So, now what wouldthis type of courses, the next 6 level courses what are we going to teach, we are going to teach what is the implication of the information security on the data owner, what is the implication of the information security on the data custodian and what is the information security implications on the data user.

If you understand all these three things properly, then developing a architecture for enforcing this information security is going to be very easy. So, understanding of this forms the crucial part of this course and that is what we will be doing.

(Refer Slide Time: 14:41)



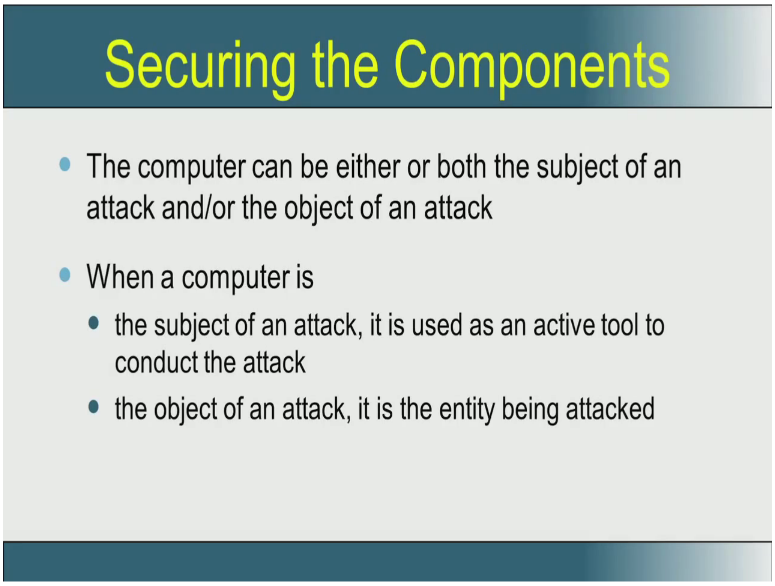
Components of an Information System

- To fully understand the importance of information security, you need to know the elements of an information system
- An Information System (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource in the organization

31

Now, what are the components of an information system? The component of an information system can be the computer hardware, it can be the entire set of software, hardware, data, people and procedures. So, it is much more than the computer hardware all that we told as tools which are needed to secure information in one of the previous slide, they comprise the information system.

(Refer Slide Time: 15:15)

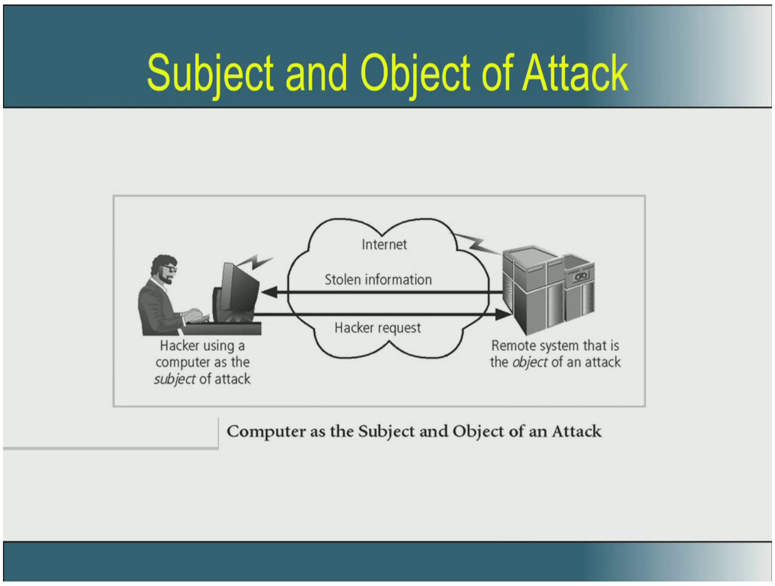


Securing the Components

- The computer can be either or both the subject of an attack and/or the object of an attack
- When a computer is
  - the subject of an attack, it is used as an active tool to conduct the attack
  - the object of an attack, it is the entity being attacked

Now, we want to secure these components, we want to secure not just the software, not just the computer, we want to secure processes, we want to secure people, we want to secure technology, what does it mean. Now, let us go component by component, let us just take the computer. Now, what I mean by securing the computer? The computer can be either or both the subject of an attack and the object of an attack. Right? So, let us go to the...

(Refer Slide Time: 15:52)



Subject and Object of Attack

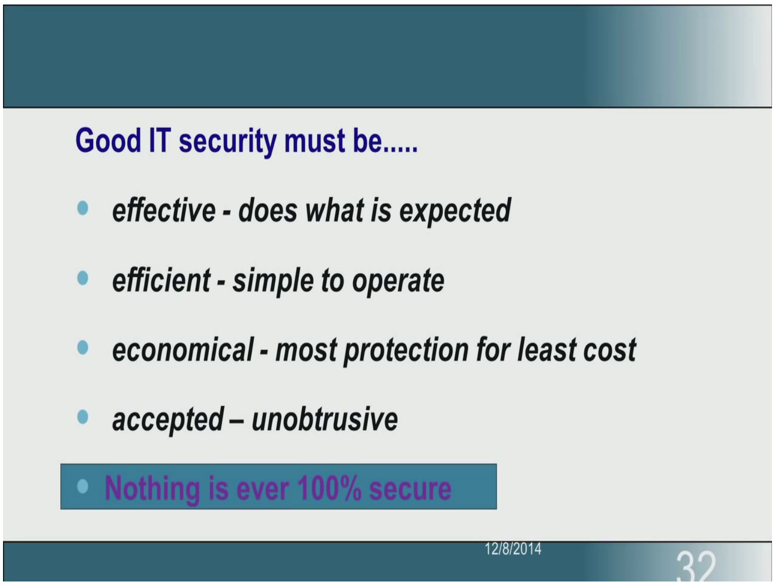
Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of attack
Remote system that is the *object* of an attack

Computer as the Subject and Object of an Attack

This is an important thing, so here the computer is actually a subject of an attack and another computer is an object of an attack. So, a hacker sits at a remote system, he goes through the internet and he goes to a server and he steal some information back through the internet. So, there are two computers involved here, one computer is where the hacker is working, another computer where which is an object of this attack, the source is this computer where the hacker is working, the object is another computer where the data is stored and he uses say an internet connection to steal this information.

Now, in a multi user system like a single server, two people can login and one can login and steal the information of the other. So, a single computer can also be an object of an attack, it can also be a subject of an attack. So, how do we secure computer, it is not that when I want to say when I... So, why I am just projecting this slide is that when I want to secure a component, it is not always that I am trying to secure it from an external object or external subject, it may be that I need to secure these components from within the system itself. So, information security when I look at security it is not just an external attacks, it could also be attack internal to the system and that is what we should keep in mind.

(Refer Slide Time: 17:46)



Good IT security must be.....

- *effective - does what is expected*
- *efficient - simple to operate*
- *economical - most protection for least cost*
- *accepted – unobtrusive*
- Nothing is ever 100% secure

12/8/2014

32

So, the good IT security essentially means that it should be effective. What I mean by effective, that is what it is expected. It should be efficient, it should be very simple to operate I can't say to login to your account, you need some 100 different authentications like you need to put your finger print, then show your eye rays, then show another password, then I have OTP and then you will get one grid and then you will have a key board on your screen and then that is all nobody will use your bank account.

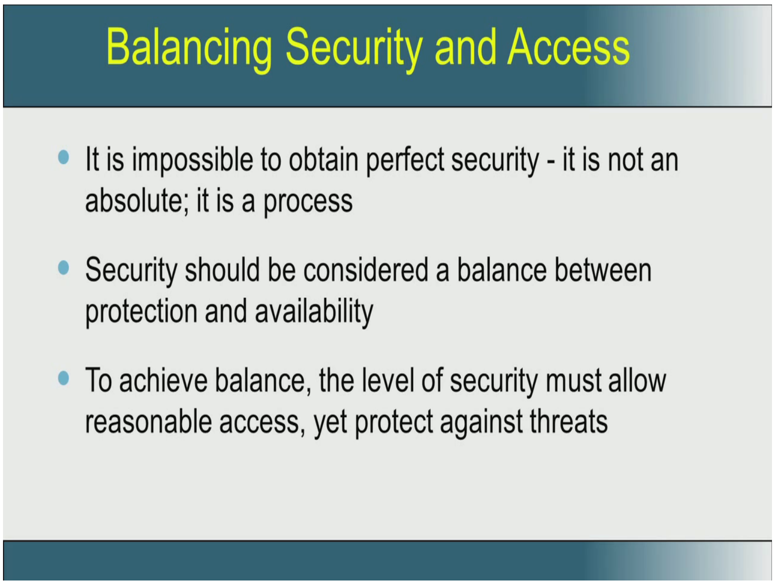
So, your thing should be simple to operate and it should be economical like, I will give you a security, I will give you a device by which there will be, we will ensure your security, but that this could be hundred thousand rupees, I will give you a USB dongle, if you put it on your computer, then all the transactions with my bank is going to be secured. But, the dongle will cost you 1 lakh, nobody will come to you.

So, it should be economical and it should be accepted and there it should be unobtrusive in the sense, your customer should accept this as I need this, why are you paining me, why are you giving all these. So, that should not be a reaction for a secure thing, so I go and say I am doing it for your security, the customer should readily accept, there is something and please understand nothing is ever 100 percent secure.

Because, still we have not understood how some body can come and steal the information, if you have understood all the ways by which some body could steal information, if you have understood that then we know how to secure. But, till today we don't know every day a new type of hack comes and so we really do not know how the information could be secure.

So, nothing is ever 100 percent secure and that should be the both all the three, the data owner, the data custodian and the data user must realize that nothing is 100 percent secure and that disclaimer should be always there in their mind.

(Refer Slide Time: 20:04)



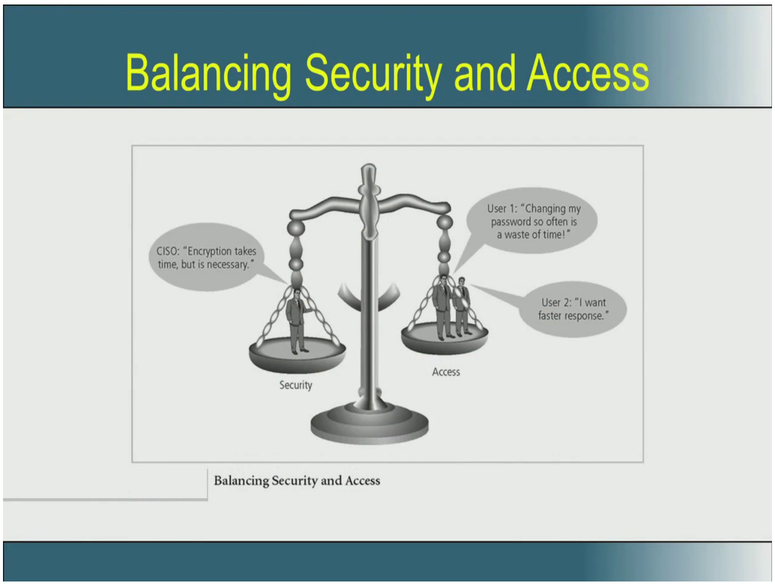
Balancing Security and Access

- It is impossible to obtain perfect security - it is not an absolute; it is a process
- Security should be considered a balance between protection and availability
- To achieve balance, the level of security must allow reasonable access, yet protect against threats

So, one of the important thing that people look at is to how to balance this security vs access. I want to allow people to access, but I want to put a security to monitor that access. The more the security I put more difficult would be for somebody to access, let us the security I put it becomes easy for somebody to access. So, the security and access to a particular resource, what are be it, are orthogonal and we need to have a balance between this protection and availability. Security essentially means protection, access essentially means availability.

So, one of the very, very important decisions that make or one of the important constituent of a information technology policy, IT policy of a company or IS policy Information Security policy of a company or an organization is how do you balance security vs access.

(Refer Slide Time: 21:20)



Balancing Security and Access

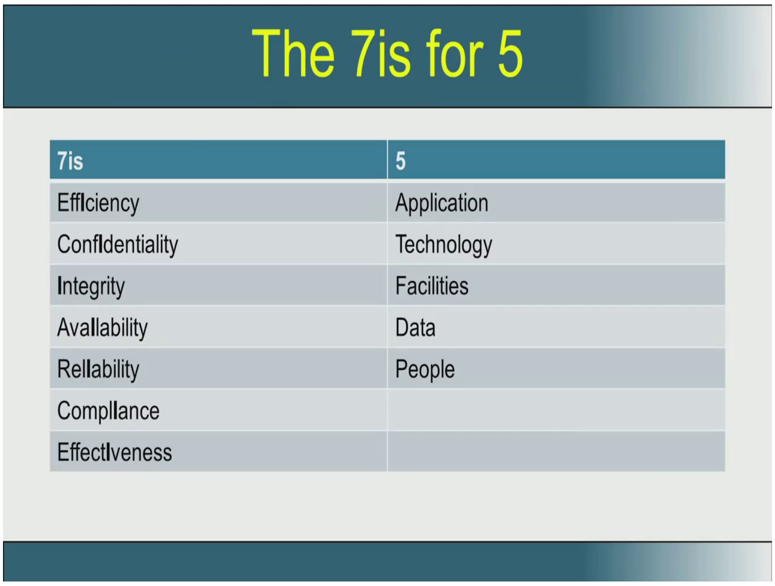
CISO: "Encryption takes time, but is necessary."
User 1: "Changing my password so often is a waste of time!"
User 2: "I want faster response."
Security
Access

Balancing Security and Access

So, this is the very nice slide from the book, the chief information security officer says I need lot of encryption, because his head is going to wrote if some information is lost. But, on the other hand user says I cannot keep changing password regularly and I want very fast response, if I start putting more and more access control, the response becomes slow. So, the user is always looking at availability and quick response and you want to finish the transaction fast.

But, on the other hand the see saw… So, the information security officer wants to put as many secure control as possible, access control as possible, so that the data is not lost. So, arriving at a balance between security and access is a very, very, very complex thing and that forms the basis of many information security, that promises the challenge of many information security policies.

(Refer Slide Time: 22:22)



The 7is for 5

7is	5
Efflciency	Application
Confldentiality	Technology
Integrity	Facilities
Avallability	Data
Rellability	People
Compllance	
Effectlveness	

So, to finish the section on the definition of information security, this is all that we want, we want the 7is is for the 5. What are though 7is efficiency, confidentiality, integrity, availability, reliability, compliance, effectiveness you see an I in each of these 7 things and we need to ensure all these 7is for each one of these 5 namely application, technology, facilities, data, people. To just elaborate a bit, I need to have efficiency, confidentiality, integrity, availability, reliability, compliance, effectiveness on the application that I use, I need to ensure efficiency, confidentiality, integrity, availability, reliability, compliance, effectiveness on the technology I used and similarly for the facilities, data and people.

So, the 7 cross 5 understanding how I can make an application, efficient from security point of view. How I can ensure confidentiality on an application from a security point of view, if each one of the 7 cross 5 factors are studied and understood, first the definition, then the process, then the education and awareness if all these things are ensured, then your system becomes secured.

Next we will deal about the 3 goals of security, now we need to define the 7is and these 3 goals namely availability, confidentiality and integrity are 3is of that 7is and we will start defining these 3 goals of security in a more elaborate fashion.