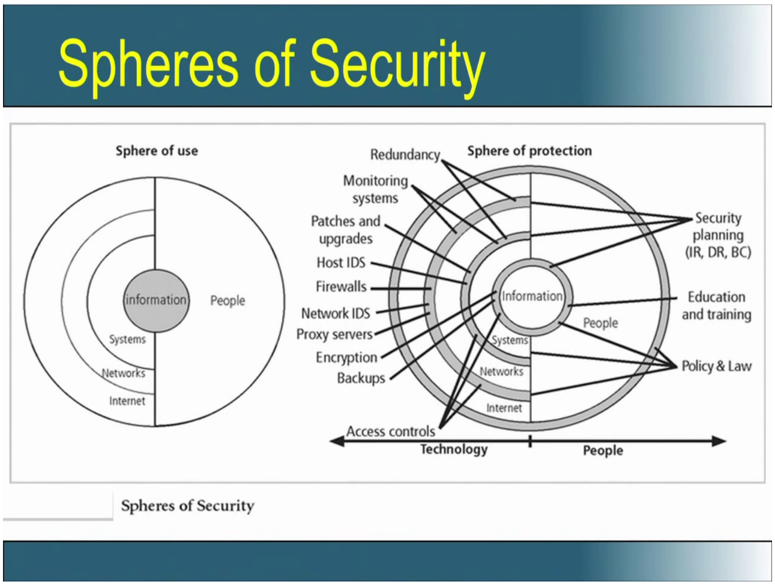
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 17

Now, let us talk about the spheres of security in more detail.

(Refer Slide Time: 00:29)



Spheres of Security

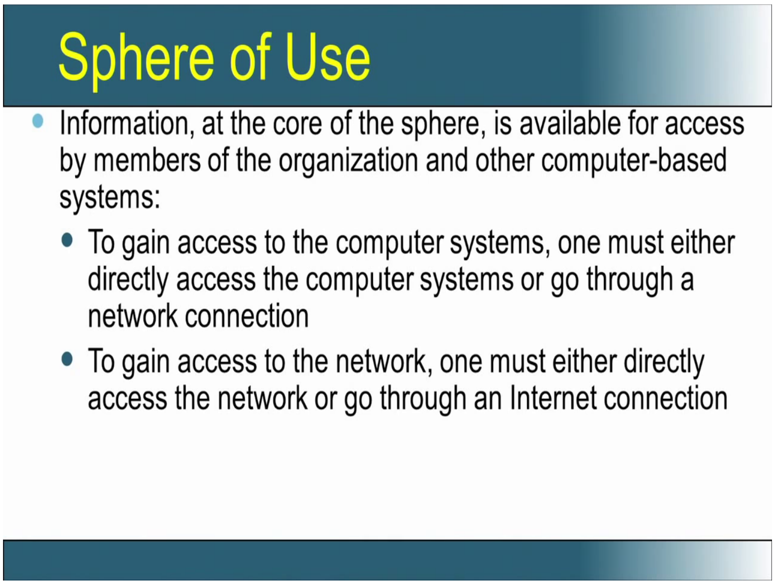
Spheres of Security

As you know there are the people are on the right hand side and the technology on the left hand side and then, you have formed three spheres, namely systems, networks and internet on the left hand side, while you see the people on the right hand side. This sphere of security forms the foundation of a security net frame work. As I mentioned information is core and it can be attacked directly by the people and it can also be attacked indirectly on the left hand side through the internet network and systems.

Now, what is very important here is how do we stop this attack. So, at every level as you see, you see a track and each track is an isolation of the internal layer to the external layer. It provides you a boundary or an isolation or what you call as an access control. You can call anyway. Now, you look at every boundary for example let us take one boundary like information and people. So, what prevents people from accessing information? It is the policy and law, education and training you give and then, the regulations that you have at your data centers, right.

So, if you look at people, the ring; the semi ring people on your right hand side and the information and if you just look at what is there on the track between that semi ring and that information, you see all the access controls and the policies. So, when I am arriving at a security policy, I should look at each one of this boundary in great detail. So, you have so many things here for example, internet and external world you have network inclusion detection system, proxy servers, encryption back up so many things that you see and lot of redundancy, patches upgrades post and IDS. So, many things that you see and all these things at a very broad outline should be part of your security, information security policy.

(Refer Slide Time: 03:15)

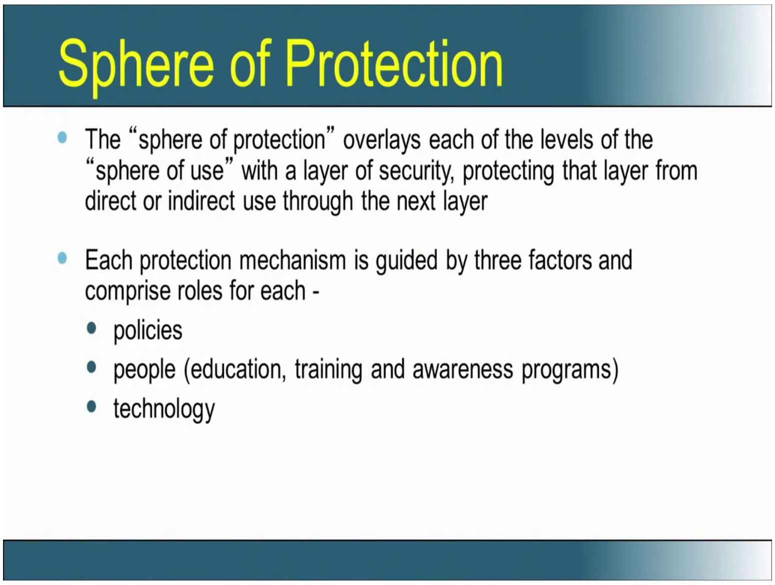


Sphere of Use

- Information, at the core of the sphere, is available for access by members of the organization and other computer-based systems:
  - To gain access to the computer systems, one must either directly access the computer systems or go through a network connection
  - To gain access to the network, one must either directly access the network or go through an Internet connection

So, the sphere of security essentially forms a very good frame work for you to start populating the policies inside your IS policy document. Sphere of security can be viewed in two ways. One is sphere of use and the next one would be sphere of protection. The sphere of use essentially says what every sphere can do with the internal sphere, with the layers internal to it. What people can do with information, what systems can do with information, what network can do with systems and what network can do to information through the systems, what internet can do through the local network, through the systems to the information? So, the sphere of use basically talks about the different functionalities, different authorized functionalities that a user, a person can do directly or indirectly or any other asset can do directly or indirectly on your information. So, that is what we call as the sphere of use.

(Refer Slide Time: 04:19)

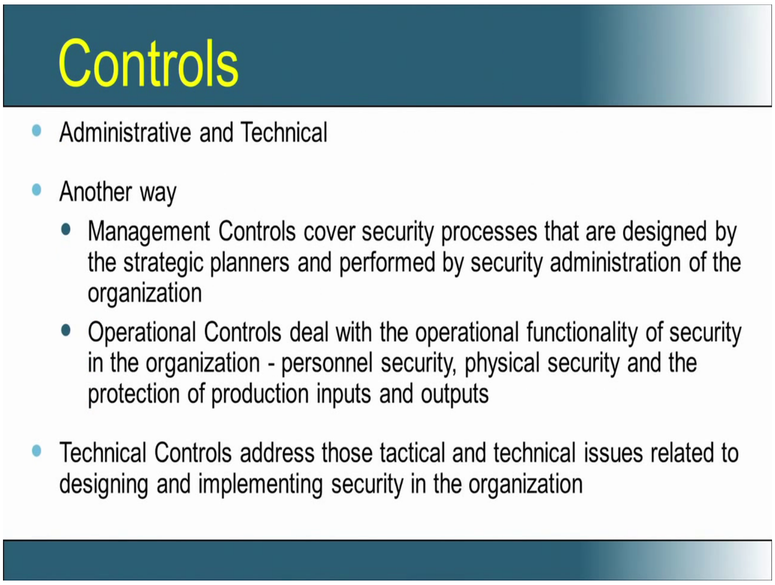


Sphere of Protection

- The “sphere of protection” overlays each of the levels of the “sphere of use” with a layer of security, protecting that layer from direct or indirect use through the next layer
- Each protection mechanism is guided by three factors and comprise roles for each -
  - policies
  - people (education, training and awareness programs)
  - technology

Now, the sphere of protection actually is over lay on this sphere of rule which basically says when you do certain actions on the information, these are the checks that need to be done for the different functionalities. Now, the sphere of protection basically is achieved by looking at people, policies and technologies who are and trying to impose access control on each one of this. So, the entire IT policy document when it is formed looks at the sphere of as look at IT sphere and then, there could be two policies that could be inferred from this sphere. The one is based on the sphere of use and another is a sphere of protection.

(Refer Slide Time: 05:10)



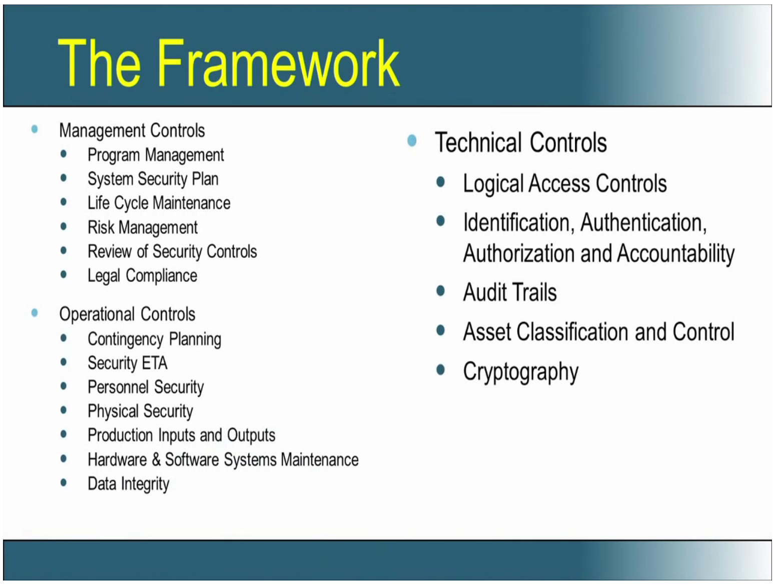
Controls

- Administrative and Technical
- Another way
  - Management Controls cover security processes that are designed by the strategic planners and performed by security administration of the organization
  - Operational Controls deal with the operational functionality of security in the organization - personnel security, physical security and the protection of production inputs and outputs
- Technical Controls address those tactical and technical issues related to designing and implementing security in the organization

So, we have already talked about controls and we did tell you that control is very important for getting the necessary or desired information, the security from information technology point of view and at that time we also talked about two types of controls, namely administrative and technical controls. Now, the administrative control, both these control should be part of your IT security policy, and when we start listing these controls, we can look at from the administrative control, we had looked at things like segregation of duties. From the technical control, we have looked at access controls; we have looked at password etc.

Now, another way of looking at administrative control here could be to divide this admin partition, this administrative control into two parts namely the management controls and the operational controls. So, the management controls actually cover security processes that are designed by the strategy planners and performed by the security administration of the organization. While the operational controls deal with the operational functionality of security in the organization, namely personal security, physical security and the protection of inputs and outputs. A very simple management control would be to say that you know this is the architecture; these are the authorized personnel who can have access to some path, right. So, it should be restricted to this. While another very simple example of an operational control would be that when you take out a system, the disk should be completely trashed, right. The disk should not go out as a e-waste, but it should be completely destroyed and only that distraction should go out. So, that is an operational control. So, these are something that goes into the control aspects of your document.

(Refer Slide Time: 07:47)



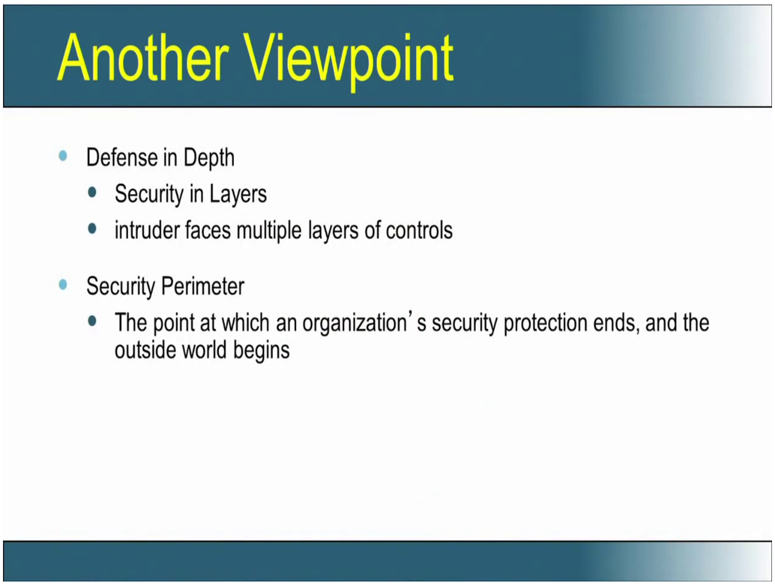
The Framework

- Management Controls
  - Program Management
  - System Security Plan
  - Life Cycle Maintenance
  - Risk Management
  - Review of Security Controls
  - Legal Compliance
- Operational Controls
  - Contingency Planning
  - Security ETA
  - Personnel Security
  - Physical Security
  - Production Inputs and Outputs
  - Hardware & Software Systems Maintenance
  - Data Integrity
- Technical Controls
  - Logical Access Controls
  - Identification, Authentication, Authorization and Accountability
  - Audit Trails
  - Asset Classification and Control
  - Cryptography

So, let us look at the frame work in a list, slide actually list all the different frame works from the control point of view. A management controls program management, system security plan, life cycle manage maintenance, risk management, review of security controls, legal compliance etc. We will look at operational controls: contingency planning, security estimated times and personnel security, physical security, production inputs and outputs, hardware and software systems maintenance, data integrity etc and you have technical controls which you have already talked of like logical access controls, identification, authentication and authorization, accountability, audit trails, log management, asset classification and control and then cryptography. So, all these are part of technical control.

So, the next thing we need to next ingredient of your security policy which will help you more on the standard. So, the policy comes out with some standard.

(Refer Slide Time: 09:03)

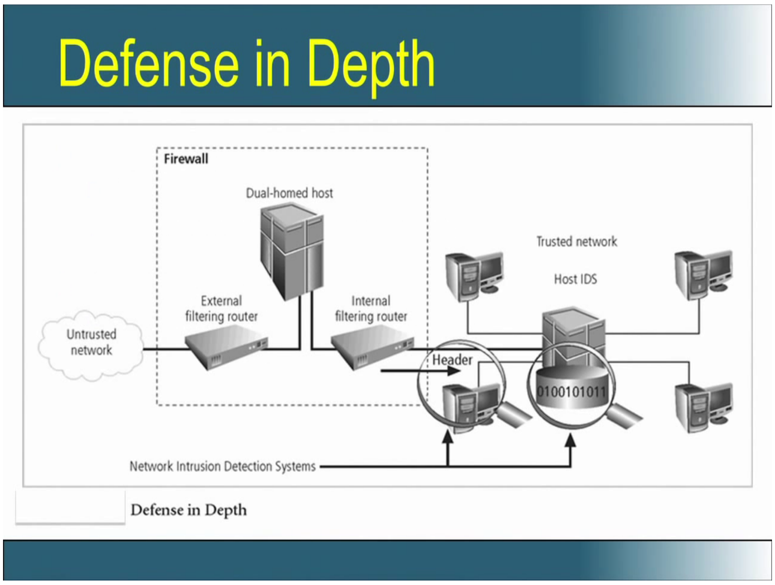


Another Viewpoint

- Defense in Depth
  - Security in Layers
  - intruder faces multiple layers of controls
- Security Perimeter
  - The point at which an organization’s security protection ends, and the outside world begins

The next thing that will help you on the standard would be these two things what we call as defense in depth and security perimeter. What is defense in depth? We will see about both of this in great detail in the next two slides.

(Refer Slide Time: 09:16)



Defense in Depth

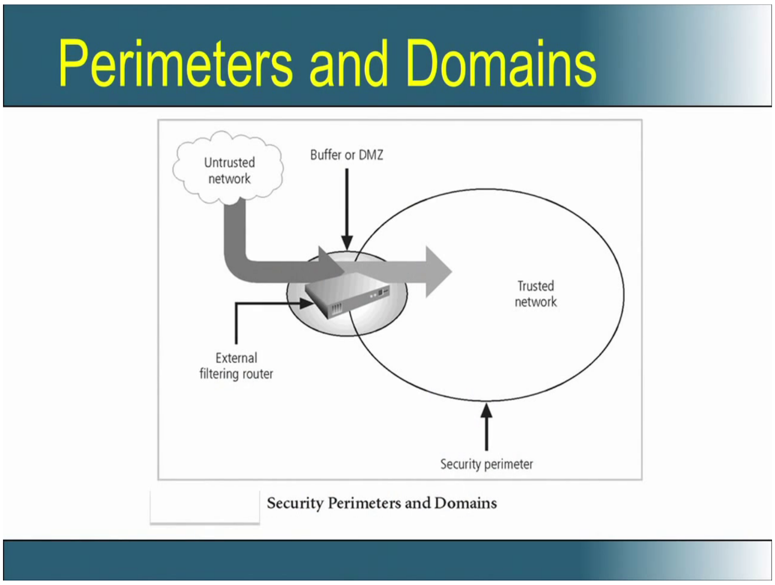
Firewall
Dual-homed host
External filtering router
Internal filtering router
Untrusted network
Trusted network
Host IDS
Header
0100101011
Network Intrusion Detection Systems

Defense in Depth

So, this is what we call as defense in depth. If an intruder wants to intrude from an external, intruder wants to intrude into your system, then he need to cross several tiers of security. For example, if we take an airport, it is actually a defense in depth as security who checks at the entry. Then, there is a check in counter which authenticates you, then there is another security check who checks all your baggage etcetera and then, there is another person who validates whether you are going into the correct plane and then, there is another security check who ensures whether you have got a security stamp, you have done the security check properly and then, when you are about to board the plane, another somebody checks your card. So, there are several layers of security that happens. That is an example of a defense in depth.

Similar thing you can see in the slide also. When I have an untrusted internet which I do not trust and then, it comes through a firewall. The firewall essentially has an external filtering router and dual on host and then, another internal filtering router. Then, it goes to a header into a trusted network. So, this is what we mean by defense in depth. So, how much defense should I have, how much depth should I have in this defense? Defense is directly proportional to depth, more the depth more the defense, but more the depth less will be the performance and more will be the cost. So, the person in the untrusted network should quickly access your data, but at the same time should be prevented from doing some undesirable actions and that is again the balance here.

(Refer Slide Time: 11:07)

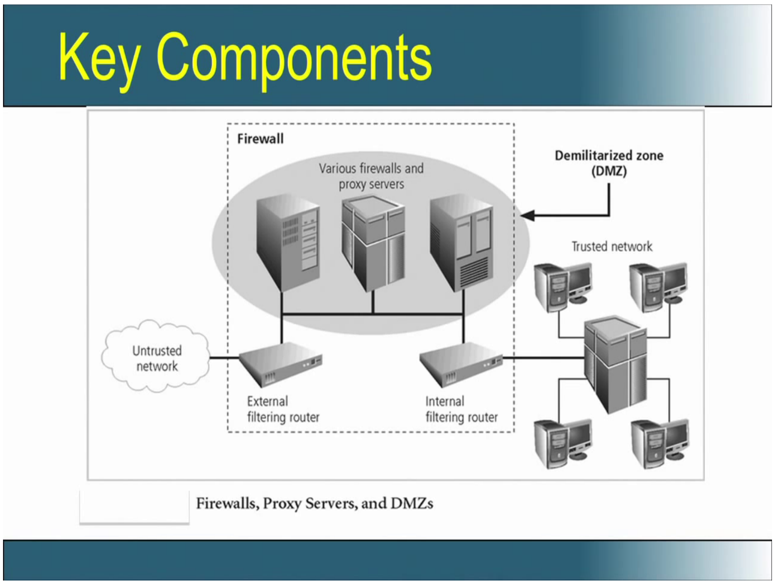


Perimeters and Domains

Security Perimeters and Domains

The next thing is about perimeters and domains. What I mean by perimeter. So, I have an untrusted network and that untrusted network or what we call as external filtering router is the interface between the untrusted path and the trusted network. So, that forms the perimeter. So, all the devices in this perimeter will partition your access phase between what you call as a demilitarize zone and an untrusted zone, right. So, what does this say when arriving at a standard or a procedure not exactly that policy level, but at the standard level or at a procedure level when I am looking at this, this at least this standard will talk a lot about the devices that are on the perimeter of your untrusted and the trusted network because that will be the most important part of your policy, a weakness there can be thoroughly made vulnerable. It can lead to a lot of vulnerability. A weakness of the perimeter can essentially lead to lot of vulnerability. So, this is what we talk of as perimeters.

(Refer Slide Time: 12:30)



Key Components

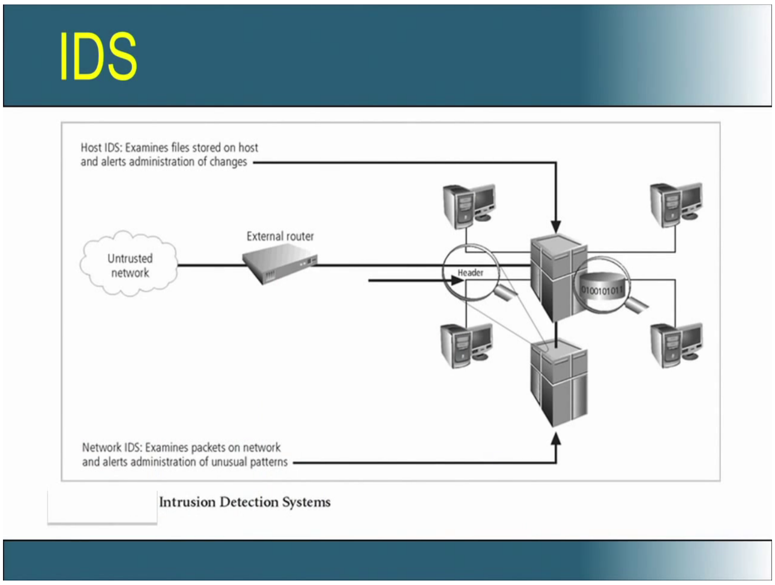
Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Trusted network
Untrusted network
External filtering router
Internal filtering router

Firewalls, Proxy Servers, and DMZs

Now, the key components that will be part of your defense and the perimeter would be these firewalls which will form what you call as the demilitarize zone, and that demilitarize zone will separate your untrusted network from the trusted network. So, you see a normal deployment in a data center where your untrusted network comes and it goes through various firewalls and proxy servers, and then there is some internal fit, both external filtering and internal filtering before you go into the trusted network. So, in this way if such a defense is available, then you are much more protected than the thing.

Another type is so we have actually seen a firewall, but that is actually different from an intrusion detection system. I just talked about in some of the earlier classes. So, what does the intrusion detection system does? It actually examines packets on network and alerts administration of unusual patterns, right.

(Refer Slide Time: 13:46)



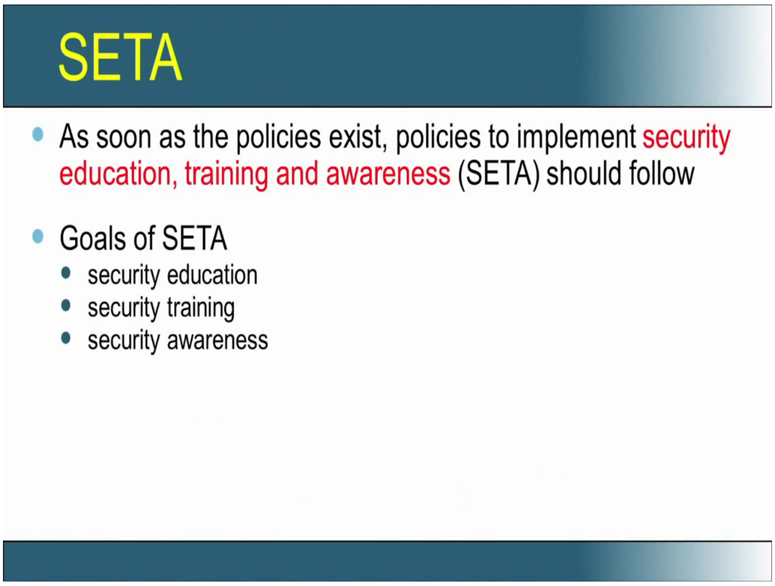
IDS

Host IDS: Examines files stored on host and alerts administration of changes
Untrusted network
External router
Header
0100101011
Network IDS: Examines packets on network and alerts administration of unusual patterns

Intrusion Detection Systems

So, there is a network intrusion detection system. There is also a host intrusion detection system which examines files stored on host and alerts administration of changes, right. So, there are two types of intrusion detection system. One is the host intrusion detection system and another is a network intrusion detection system and each does different functionality, but please do understand IDS is different from firewall.

(Refer Slide Time: 14:19)

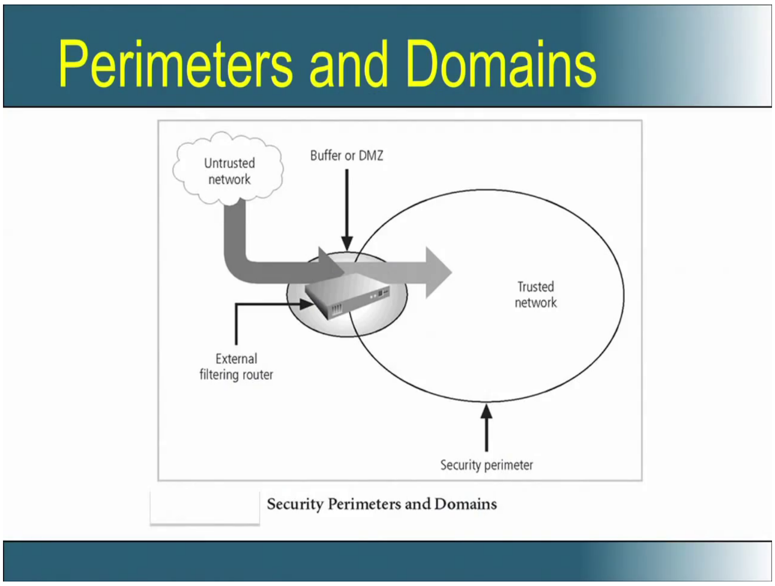


SETA

- As soon as the policies exist, policies to implement security education, training and awareness (SETA) should follow
- Goals of SETA
  - security education
  - security training
  - security awareness

So, the last part of what should be inside your information security policy is what you call as the SETA. What is SETA? This is nothing, but Security Education Training and Awareness and the goals of this SETA should be to educate the employees on security, should train the employees on security, and should create an awareness of the employee on security. So, what is the difference between education, training and awareness? This is very important because if people are not people, process, technology, they form the foundation if people are the most important vital asset that you have and that asset is not, people are one of the most important defense that you have against external attacks and if in the sphere if you see people do matter quite a bit and if this people, the ring that you put around the people. So, let me just go through the slide.

(Refer Slide Time: 15:28)

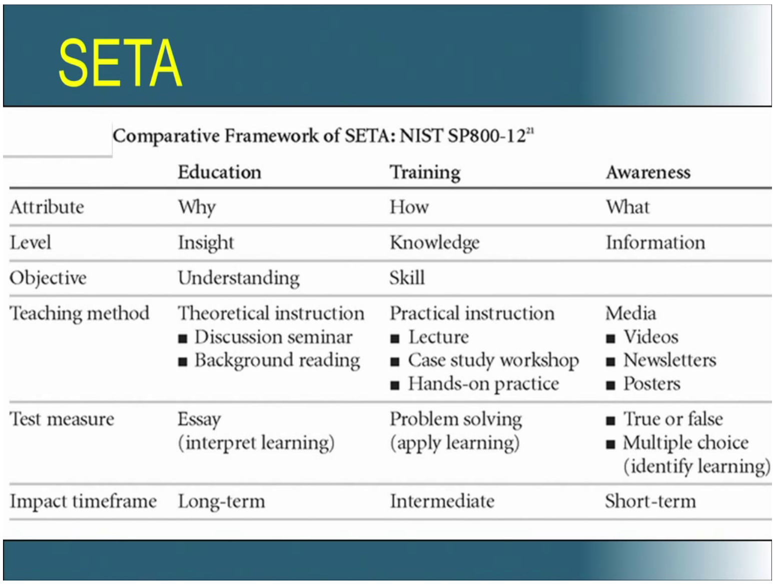


Perimeters and Domains

Security Perimeters and Domains

For outer most ring that you put there, right and the inner most ring between the people and the information, please note that education and training form part of both rings and if you are not going to train these uses, they are going to cost big vulnerabilities in this. So, just to emphasize that continuous education, training and awareness on information security is a must for every HR should note this, every HR of all organizations which are IT driven should take this point very seriously and it should be part of your academic calendar. I think at least with banks, I am sure the Reserve Bank does talk about documenting schedules of how people are trained in information security. So, that is very important.

(Refer Slide Time: 15:47)



SETA

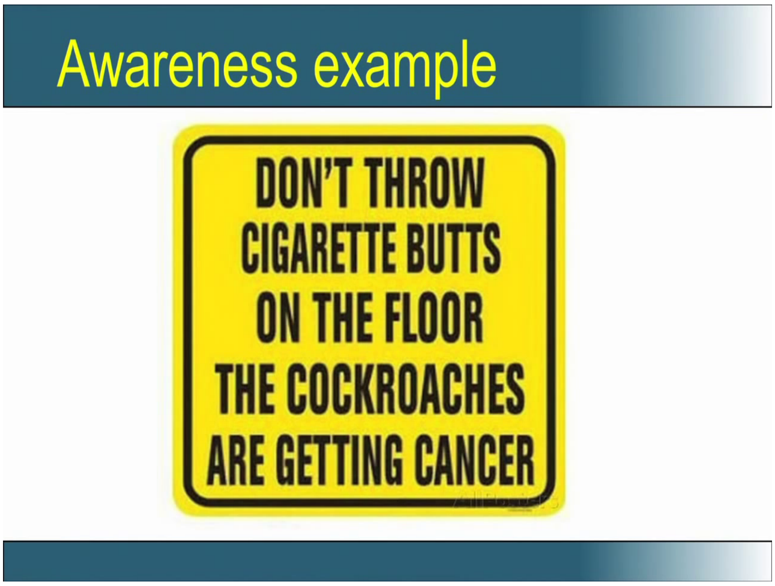
Comparative Framework of SETA: NIST SP800-12[21]

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	
Teaching method	Theoretical instruction ■ Discussion seminar ■ Background reading	Practical instruction ■ Lecture ■ Case study workshop ■ Hands-on practice	Media ■ Videos ■ Newsletters ■ Posters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	■ True or false ■ Multiple choice (identify learning)
Impact timeframe	Long-term	Intermediate	Short-term

Now, we have talked about three things. We talked about education, training and awareness. What are the differences between this? So, this is a very nice frame work. I just leave it for you to just go through this by this is being run by NIST. So, in education we talk about why we want to have information security, but training we say how do you achieve this. Awareness you say what it is, right. If somebody is educated, information security he has an insight into the problem in training as knowledge to this problem. In awareness he has some information about this problem. The objective of education is to make the fellow understand this. The objective of training is to create a skill set. Objective of awareness is to just to see who is aware. There is no objective of that. It is just that you make person aware of that. So, in education we have theoretical instructions which come out of these types of lectures, discussion, seminars, background reading. Training again it is lecture, case study, workshops and some practice. Awareness is just videos, newsletters, and posters.

In education, we have that way we test understanding is by essay, interpret learning, how we have interpreted it. In training we say how it is applying, what he has done. In awareness, it is just multiple choices. So, again education will have long term impact while training has intermediate, while awareness would have short term. Why I spend more time on this slide is to just basically tell you that the six levels of courses that we are offering is going to address education, training and awareness. So, the first level would be more of between awareness and training, right and the bit on education. As slowly as we go to the next stage, it will be more of training and then the little more on education. As we go to level 6, it will be lot of education. So, that is how we have also structured these 6 levels of course.

(Refer Slide Time: 18:51)

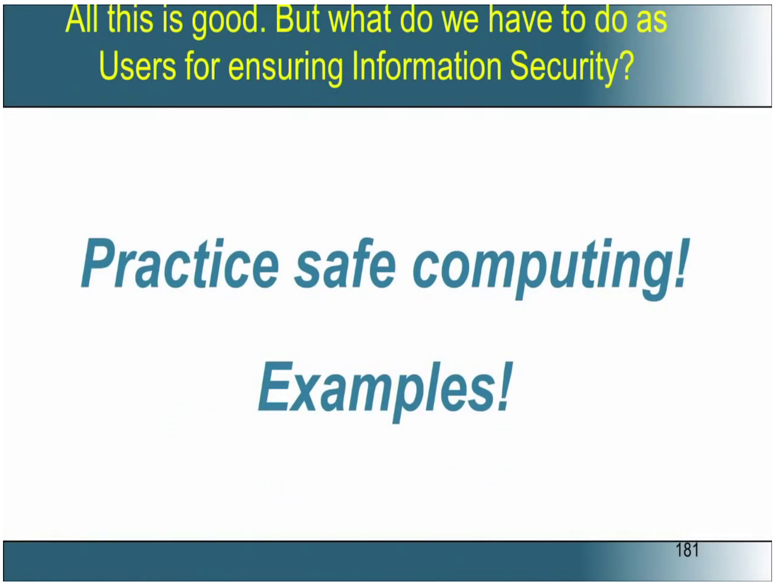


Awareness example

DON'T THROW
CIGARETTE BUTTS
ON THE FLOOR
THE COCKROACHES
ARE GETTING CANCER

Now, there are very just to add some have been talking a lot of technical things. This is a very interesting awareness example. I leave it for you to see in laugh over and also search barrel. Do not throw your cigarette butts on the floor.

(Refer Slide Time: 19:09)



All this is good. But what do we have to do as Users for ensuring Information Security?

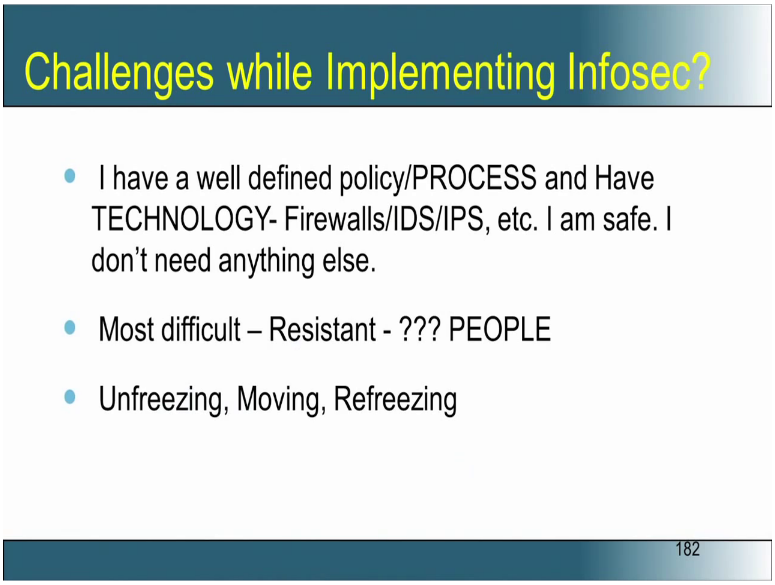
Practice safe computing!

Examples!

181

So, the last two minutes I will be spending to tell you again going back to the introductory speed. We as technologist or computer scientist or trainers can only build dams; can build these technologies, but to fill it with water is the owners or the people who are using this. So, it is very important that people get educated, trained, make aware and trained and educated on information technology, so that they use it properly. So, everyone who is attending this course should practice safe computing and I will give you some examples.

(Refer Slide Time: 20:01)



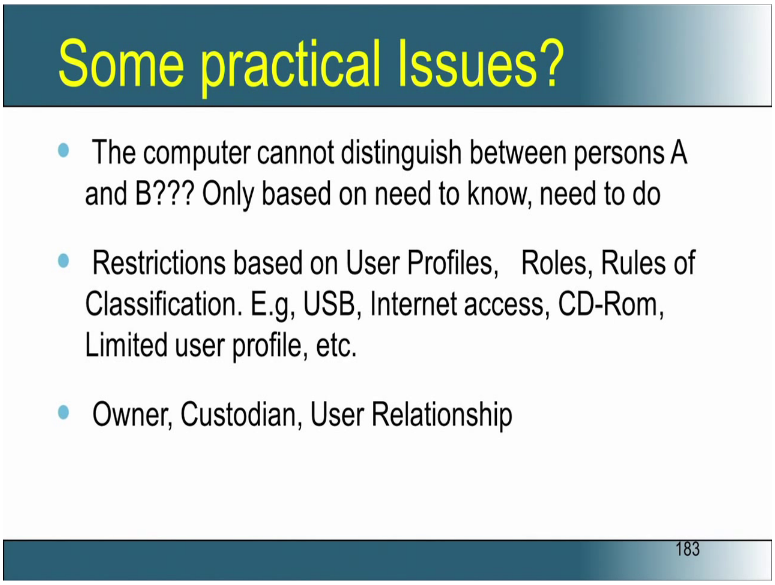
Challenges while Implementing Infosec?

- I have a well defined policy/PROCESS and Have TECHNOLOGY- Firewalls/IDS/IPS, etc. I am safe. I don't need anything else.
- Most difficult – Resistant - ??? PEOPLE
- Unfreezing, Moving, Refreezing

182

I have the best challengers while implementing infosec. I have best firewall have insisted. Still I cannot do I am not getting that security. Reason is people and the challenge here is people have to be unfreezed. They have some notions of security that needs to be as technology changes as threat models changes, right. If the people have to be unfreezed, then they have to be set moving and then, they have to be refreezed with the new technology. So, that is the challenge here. It is not that if people are consistently moving with the technology, then there is no issue, but what happens is typically in this we have sudden bout of attacks. So, people are already set for something, they are doing those. Now, we need to change to adhere to this and this change is not if they are freezed on something. So, we go and unfreeze them and then we make the move and again we refreeze them. Why should we freeze them is because we want to follow rules. The moment we want to follow rules, we want to make somebody adhere to rules and then it is necessary that we freeze them on those concepts and this is the biggest challenge in implementing information security.

(Refer Slide Time: 21:14)



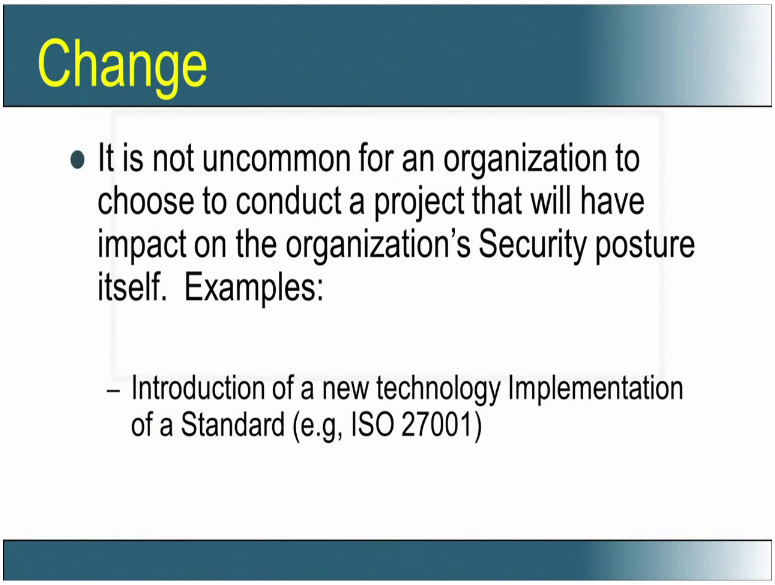
Some practical Issues?

- The computer cannot distinguish between persons A and B??? Only based on need to know, need to do
- Restrictions based on User Profiles, Roles, Rules of Classification. E.g, USB, Internet access, CD-Rom, Limited user profile, etc.
- Owner, Custodian, User Relationship

183

Then, the other practical issue is that never think that the computer can do everything. Again people matter quite a bit. Computer cannot distinguish whether I am logging into the system, Kamakoti is logging or Dilip Ayyar is logging into the system. It actually has it is based on some need to know and need to do principle. It has all these restrictions everything, but the notion is Kamakoti has to be very you know strict and secure, so that he does not give the password to Dilip and enable him to enter the system. The system will only see the login; it will not see the person unless you have biometry and another thing, right. So, these are the things that we need to be careful and still we have mentioned in this module, everything is password driven. Even you know you have even hardware security token, I can give the security token to Dilip and still he can login as minute. So, unless I put some discipline, I practice this complete understanding and I practice, I understand the implications of train to share some credentials of main with others. Thus getting a good security system is a difficult task.

(Refer Slide Time: 22:32)

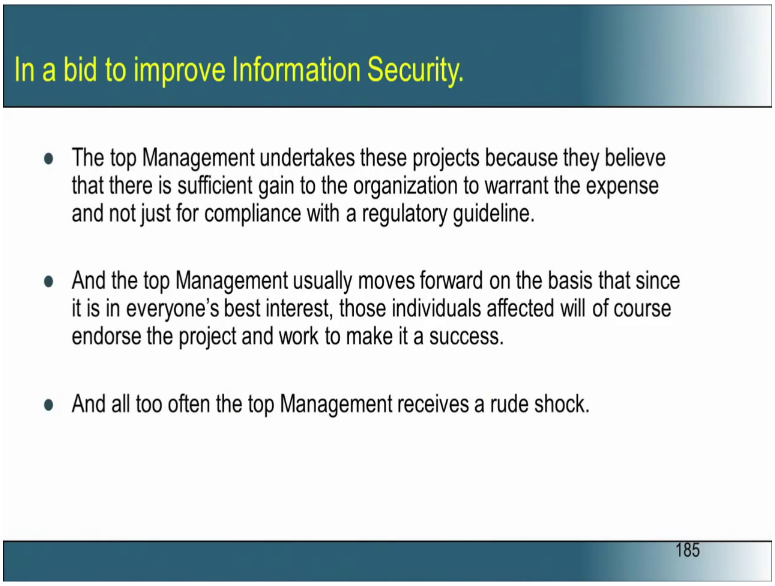


Change

- It is not uncommon for an organization to choose to conduct a project that will have impact on the organization's Security posture itself. Examples:
  - Introduction of a new technology Implementation of a Standard (e.g, ISO 27001)

The next thing is change, it is not uncommon for an organization to choose to conduct a project that will have impact on the organization security posture itself. For example, Introduction of a new technology implementation of a standard, for example ISO 27001 . So, at least such types of drills are done, but it needs to be done in a better perspective.

(Refer Slide Time: 22:58)



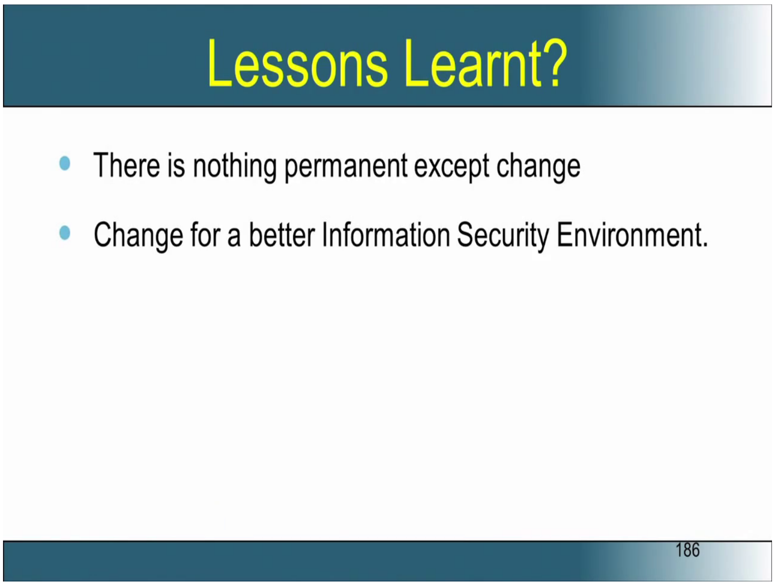
In a bid to improve Information Security.

- The top Management undertakes these projects because they believe that there is sufficient gain to the organization to warrant the expense and not just for compliance with a regulatory guideline.
- And the top Management usually moves forward on the basis that since it is in everyone's best interest, those individuals affected will of course endorse the project and work to make it a success.
- And all too often the top Management receives a rude shock.

185

These types of exercises should be done with a genuine interest to improve these stature of your organization and not just as complaints with a regulatory guideline. RBI said this should be done, so I am doing is wrong. I am doing it for the benefit of my organization and it is incidental that RBI takes a note of it, right. So, that mind set has to come and this type of the management usually should move forward on the basis that since it is in every ones best interest that everybody should endorse for this project and they should make a very consistent attempt to see that these people are well trying and the policies are correctly implemented and that often helps. Otherwise, when there is a root shock in terms of a big security lapse and that will never be thanks giving day for the organization.

(Refer Slide Time: 24:09)



Lessons Learnt?

- There is nothing permanent except change
- Change for a better Information Security Environment.

186

So [FL] brothers and sisters we come to the end of this module 1 and one thing that you would have realized the errors in information security, there is nothing permanent except change and we have to change consistently to keep changing ourselves for a better information security environment. We will now move to module 2 in the next session, where we will talk more on these policies. Thank you. [FL].