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

Lecture – 16
Introduction to Information Security

The next thing that we should do is to manage these policies. There will be revision one, and then there will be a regulatory requirement. So, you go and change the policy. So, the policies will keep on changing over a period of time. Now, when a policy changes, the challenge is the corresponding standard that it drives should change and the next challenge is that standard will imply a change in the technology or process or training. So, a policy change will have a series of impact on the standard and then, on the procedures.

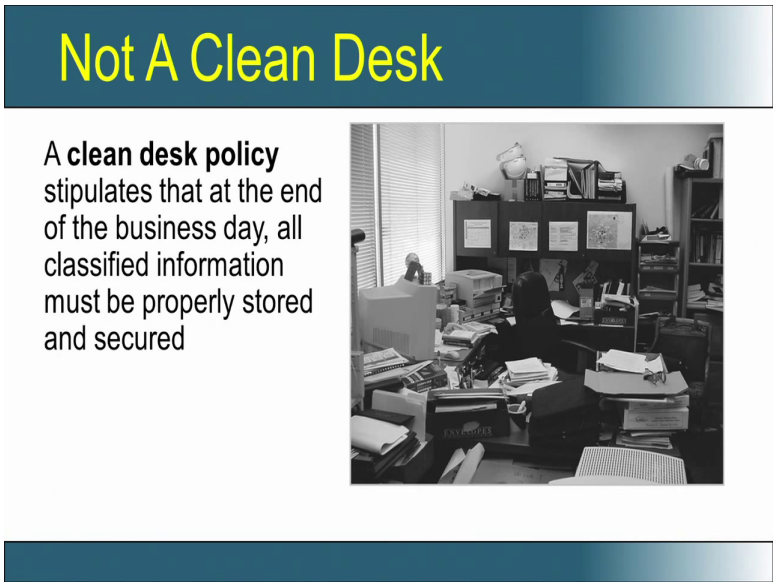
(Refer Slide Time: 00:44)

So, to track all these changes, there we need a very clear policy management perspective. Of late you actually have something called automated policy management that will meet certain specific technical control needs, etcetera. So, there is one complete technology involved or some very interesting computational problem involved of how to do version control of these policies track changes. We will talk about some of this. It is not just for an information security course, but it is also for any software development course. So, lot of principles of software engineering are basically included to basically manage policy and basically revision controls, but from the information security point of view, what I

would like you to understand is that a change in policy essentially implies a change in standard which in turn implies changing the procedures and processes.

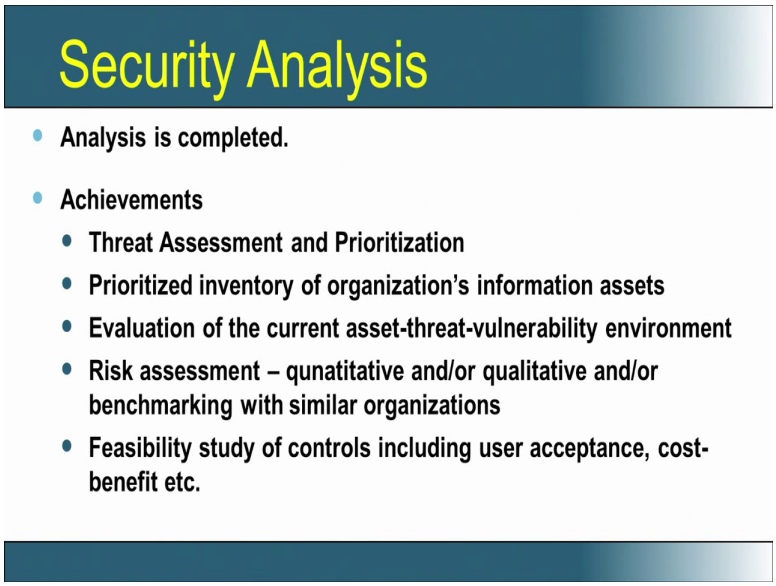
A change in the policy will not have an instantaneous change in the standard. It will take some time for the standard to evolve to meet the policy and then, it will take many more months to get an implementation or a process which will adhere to that standard. So, from the date of change of policy for its impact to reach the end, it will percolate to standard and then percolate to the process and technology, it will take months. So, all this needs to be tracked and that is a big challenge, but one very important thing that we miss, right many of us miss, and that becomes extremely important is this one thumb rule which every organization should follow which is called a clean desk policy.

(Refer Slide Time: 02:46)



A clean desk policy stipulates that at the end of every business day, all classified information must be properly stored and secured. If it is just papers, you have to put it in a safety locker, but if you have information asset which is not just paper, it is data, it is stored in magnetic medium or these things should be backed up. So, that is one of the reason why there is something called end of day. What is end of day? So, end of day is to, it has been done for long time even before information security was defined, when banks existed. Banks exists for 200 years now. They would have an end of day, but from a security perspective which is just to say that all the transaction I did today, the maker and the checker have looked into it. That is what an end of day today assures you. That itself is a clean desk policy. The figure I just put that entity, the photo there which demonstrate that it is not a clean desk, right.

(Refer Slide Time: 03:53)



Now, what we have done so far? We have done till this module, we have done what we call as a security analysis. What does the security analysis do? The achievement of the security analysis is, it does a threat assessment and prioritize these threats which should come before what, prioritizing of inventory assets of your organizations. This is more your classification of information is an example of priority and then, you have an evaluation of the current asset-threat-vulnerability environment. I have an asset and it has a threat, how much exposed is this asset to the threat is what we call as the vulnerability and then, we did something called a risk assessment which is a quantitative and/or qualitative and/or benchmarking with similar organization.

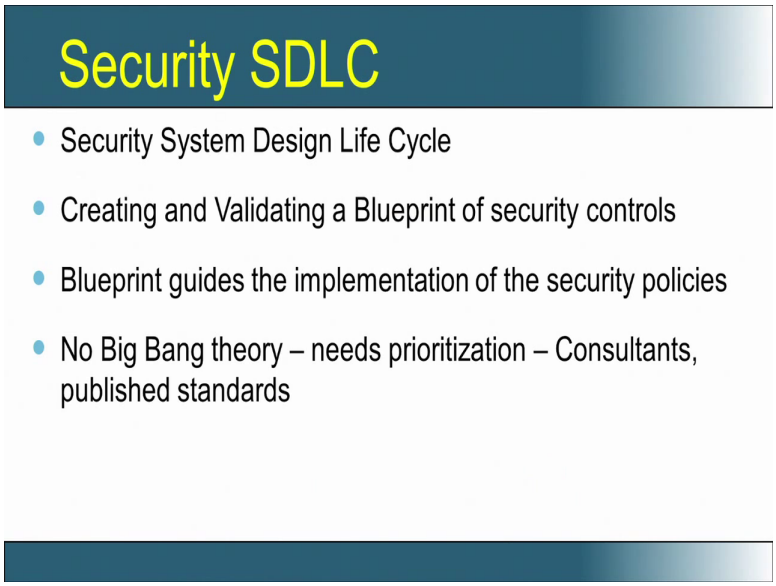
How do you asset risk? We do some quantitative analysis on the environment, on the cost as what will happen if I go. Risk assessment for a normal banker is when I give loan to this fellow, what risk I am in. So, he does a quantitative analysis. He looks at his balance sheet. That is the quantitative analysis. Qualitative analysis is very interesting here. So, you look at the domain to which he belongs to. If he is doing some infrastructure project and today country has some issues with infrastructure, or the region has some issues with infrastructure, there is no land availability, right. So, then this is a high risk. Even though his balance sheet is good, the quality of the job that is trained to perform is not conducive at that point of time, right. So, you do a quality, but today maybe steel is going very fine. So, you go and if you go and start funding project in steel and also, you start benchmarking with similar organizations. Normally you see like if look at you know the announcements or analysis that you do in risk management, how do peers figure here.

So, we just look at general risk management meetings in many organizations. So, there is the assessment of the risk will be in three fold. One thing is quantitative, another is qualitative and another is also to benchmark with similar organizations. The way you do security, also should be like this. I should benchmark with my peers, what my peers has done.

Again I come back to one very important matter that we have been discussing in this course in a great detail in the past in the previous lectures about acceptability. I put a secured measure. I say you need some 20 passwords before you do a transaction. If I assure, every customer will move their account in the next possible day. So, there is something called a customer acceptance vs the security you should get the balance between the acceptance and the security level. How do you basically gauge this acceptance? If I put the security measure, will my customer accept it? The very quick answer for this is intelligent organization see if a competitor has put this type of thing and go to the customer of the competitors and say, hey are you feeling comfortable? Just get informal thing and that will be a great pointer for you to adopt that security measure for your organization.

So, benchmarking with similar organization forms a very important part of your risk assessment and in this also organization especially involve in IT security should come out very freely about all the vulnerabilities and the threats they have faced and attacks they have face, so that it should be a collective learning and it will form a very good input to the risk assessment. The last of this security analysis will be to look at feasibility and there already I talked about user acceptance and other thing is cost benefit. If I install the security measure, then for say a 1 million rupees and if it is going to protect me from a fraud which can happen, say once in a year and the cost of the fraud is say 20000 rupees, no bank or no organization would like to have this, right. So, even for the software vendors, the way they put the prizing is to first carefully study the cost benefit.

(Refer Slide Time: 08:47)



Now that we have this analysis is over, so we are ready with the analysis and these are all going to come and become the part of our policies. Now, the most important thing that comes out next is what we call as the security system design life cycle.

Now, the first step that you take in the security system design life cycle is to create and validate a blue print of your security controls. So, this blue print is what we call as the standard. We have talked about policy documents. Now, we are going to talk about standards. What will the blue print tell you? The blue print will guide the implementation of the security policies and another thing that many organizations should keep in mind is that the security is not just a one night affair; it is not that tomorrow morning everything would become secure. It is no big bang theory. It needs prioritization and there should be some prioritization should be based on advices that you get from experienced consultants, and it also means that you also look at lot of public standards. Already we told one thing in the context of having a two way authentication using an hardware token, and we also saw that the token were say something likes each token would cost Indian rupees 400 for 5 dollars in the US currency something like that.

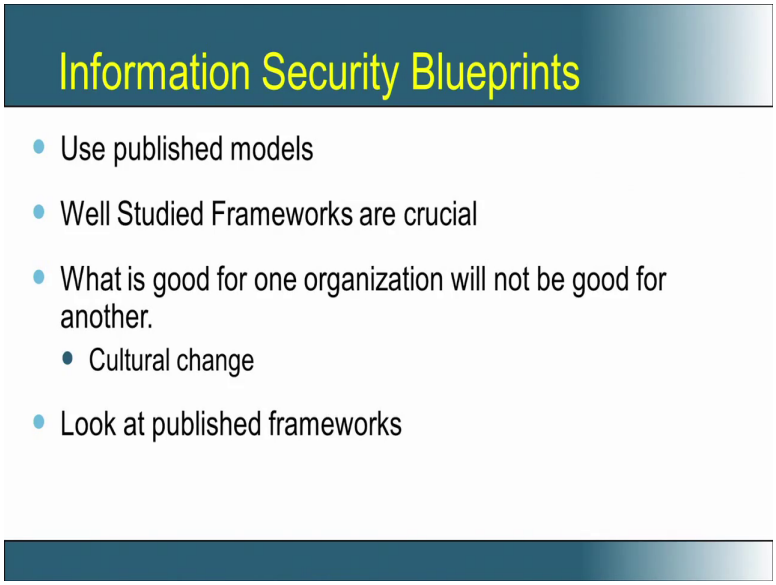
So, when I want to say when I have a organization of 20000 employees, for me 400 rupees per employee would be a big investment. So, there we need prioritizations. Some employees get today, then slowly some of us get tomorrow and some need not have this. So, security software system design life cycle is a very, is a process that needs to come out of very deep thinking.

So, now, we will talk about information security blue prints. These are all published models and we have to look at frame works that are well studied. Please also note that what is good for one organization will not be good for another because there can be say I will again go back to banking. We have an old bank that is 100 years old or 150 years old. There can be a new bank that has cropped up say since last 10 years. The customer profile itself will be different. I could have has suppose I am handling an old bank. I could have customer who do not want to change their account number for sentiment reasons.

Such type of sentiment you may not find in a young person. So, you will say though today a regulator wants a 15 digit account number and looking at the account, I need to have complete information of which branch it is, some DNA about the account, or it is a current bank, savings bank extra, but my customer can come and insist that I do not want to change for numerology reasons. I got lot of profit after I got this account number. He can come. It is not a very strange request. So, now you have to have a policy by which some have a 15 bit virtual account number for him and whenever he enter this 5 digit, it should get translated into the 15 digit. So, his five digit account number becomes virtual account number from a systems perspective, it gets translated to a physical account number.

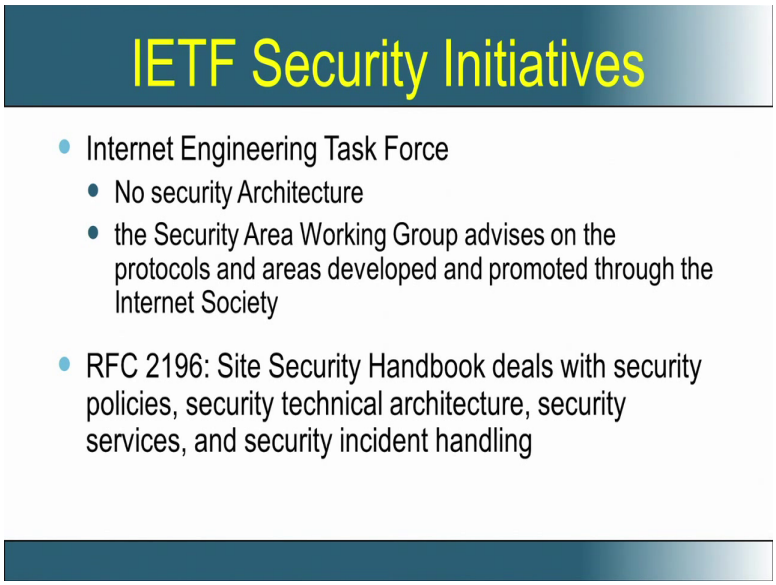
So, this is just an example, but there can be many more sensitive examples that we could give what is good for one organization need not be best or good for another organization. So, there is a cultural change.

(Refer Slide Time: 13:10)



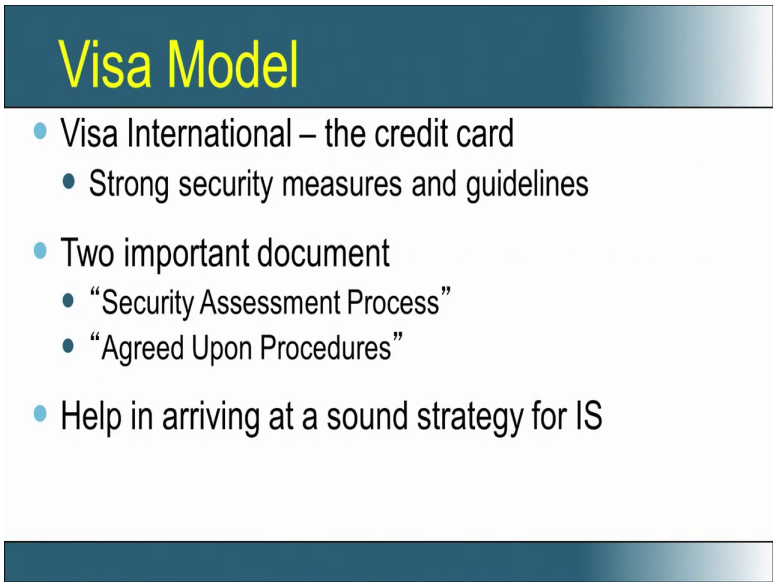
So, we need to have an information security blue print and we cannot just blindly adopt some blue print, right. If you do so, then we may be in problem. We have to carefully study this blue print and then, come to the conclusion what is much suited for my organization. So, in this context start with publish to blue prints frame works and go and modify it to suit my need. So, to tell it in, you need to buy slipper that fix your leg, rather than cutting the leg to fit the slipper you have bought. That is essentially the maxim that you need to keep in mind when you are going to evolve standards from the policies. Now, we will look at some of policy published frame works.

(Refer Slide Time: 14:12)



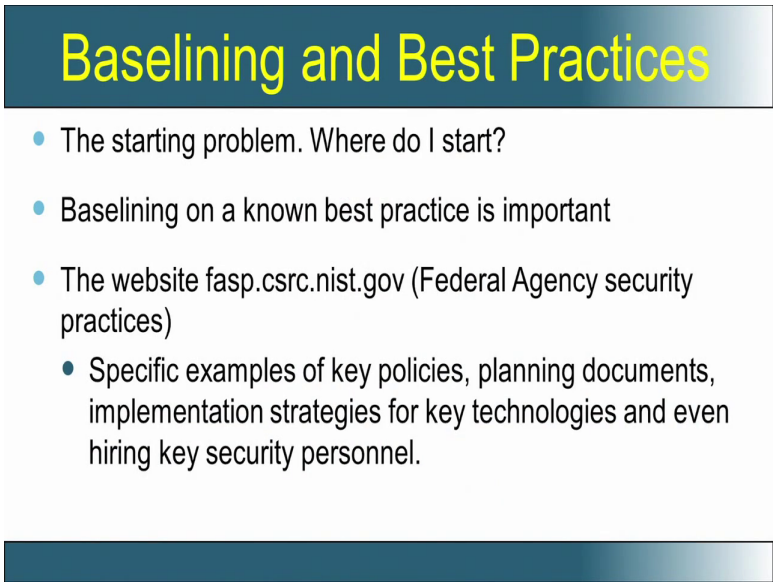
For example, the IETF security initiative is a very interesting frame work. IETF stands for Internet Engineering Task Force. No wonder these are the fellows that start looking at security because the vulnerabilities, they start at through internet. So, there is a security area working group. It actually gives advices on the protocols and areas. So, they also give some policies and we have to incorporate some of these policies into your policy document and then, use the blue print to come and implement these policies as standard. So, the RFC2196 that they have is a site security hand book. They deal with some of this frame works like security policy, security technical architecture, security services, security incident handling. They start talking a bit more about standards and procedures; not only the policy. So, IETF is one thing that you can look up when you are trying to evolve Information security policies standard and process for your organization.

(Refer Slide Time: 15:26)



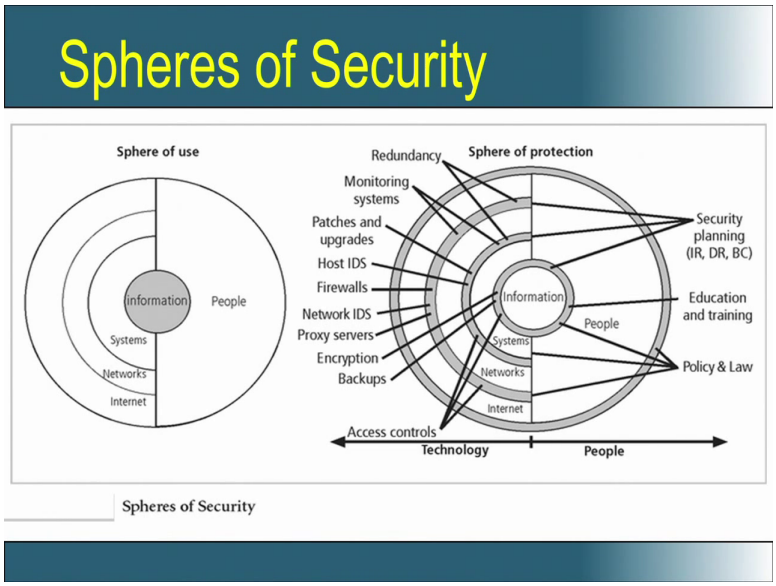
The Visa model is a very popular model. Almost all of you have as basically for attending this course, you should have a credit card. They have a very strong security measures and guidelines, right. If you actually see the number of credit card crimes Vs the total number of credit cards in the world, it will be minuscule. The ratio would be minuscule. So, it essentially proves that the visa model is indeed strong and it has looked into lot more details. So, two important documents form part of your visa model that is the security assessment process and then, agreed upon process. I leave it to the viewer. We will deal about these processes in some other later part of this, not this course with the level 2 or level 3 courses, but these sound strategies are very interesting examples. Please note that these policies are already implemented on field and they are tested on the field. It is not on paper, but it is on field and these will certainly help in arriving at a sound strategy for your information security of your organization.

(Refer Slide Time: 16:50)



So, where do you start, right? So, now, you have some frame works, you have some policy, you have understood what are all the different things that go into a policy, you have some frame works by which you can bring standards and procedures. Now, we could have some more hand holding to start. So, the starting problem is where do I start? So, base lining is one very important thing. The website, the federal agency security practices FASP website is a very interesting website for everyone to look at and this can basically guide you on the first statement that you can put on your policies, then your standards and then your procedures. So, they give you specific examples of key policies planning documents implementation strategies for key technologies and even things like hiring key security personal. Note information security is not just technology; it is people, process and technology.

(Refer Slide Time: 17:59).



Now, we will look into what we would achieve and what are the guiding factors of arriving at an information technology, policy, standard and processes? At this point I will just end this session with what we term as spheres of security. We will continue more about this in the next session, but before I end let me tell you that the spheres of security has the most important stuff. The nucleus which is the information and around that you have people who directly access this information, those are the internal people to your organizations. So, we go back to our people, process, technology that people are very important. That is what this spheres of security tells you. On the other hand, we have methodologies which give people an indirect access to the information, namely through your internet, your networks and the system.

So, there are people who have direct access to your information and they are basically the custodians of your data. There are people who can access your information by maintaining through the systems, through the networks and also through the internet. Systems are people who maintain, they are also custodians who have access to the direct access to the systems. There will be people who can access to systems to a network. For example, if you take a bank people sitting on the branches, they come to access the information to a network internal network and then to the system, then to the data base. Then there are external customers of your bank who do internet banking; who come through the internet into your network, then into your system, then into your information. So, when I look at arriving at a information security policy, I should look at all these spheres, people who actually maintain the data, the custodians of the data, people who

actually does some operations like back up etc, who have direct and indirect access to your data base through systems, then the users within your organization, your employees who access this information from the network, through the network, through the LAN through the systems, then to the data base and then your external customers who access your information through the internet, through your local network within the data centre, then into your system, your application server, then to the data base. So, we will look more about this spheres of security in the next session.