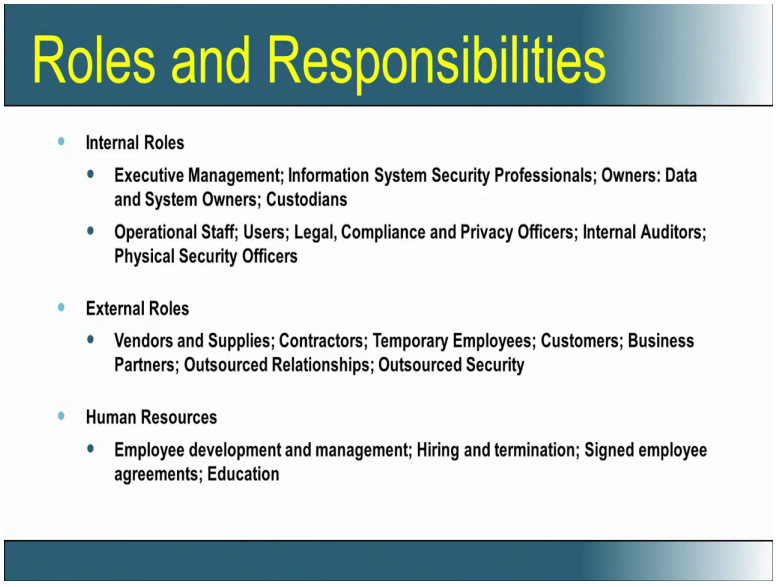
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 15

(Refer Slide Time: 00:10)



While we are arriving at a security policy, information security policy. We have now talked about classification of information earlier. Now, we should talk about roles and responsibilities. Now, again there is a classification that we need to do at the roles levels. So, there are there are internal roles, there are external roles, and then there are human resources. So, what are the internal roles? People internal to the organization, what are the roles? People external to the organization what are the roles, and what is the role of a human resource. The roles also come out with responsibilities. Now, let us go and look a little more into a internal roles. The internal roles actually comprise the executive management and the operation staff. The executive management will have also the information system security professionals, the owners of the data and system, and the custodians of this.

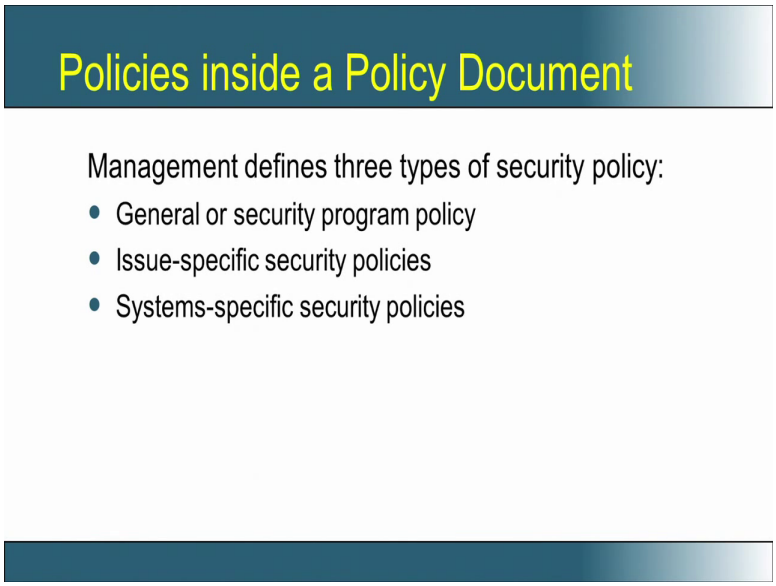
So, these are all the part of your one class of internal roles we can say. And all of them may be monitored directly by the executive management. Then there are the operational staff, which is another category, which includes the users of the assets; the legal complaints and privacy officers, the auditors, and a physical security officers. So, the internal people within the organization may be classified from the responsibilities and roles from the information security perspective into these two as we have seen in the

slide. the external people are the vendors, suppliers, contractors, temporary employees, customers, business partners, outsource relationships, outsource security, all these things they are all these people, are the external partners, external people, and their roles and responsibilities also need to be fixed. The role of the human resource within an organization, is to come out with employee development and management. The hiring and termination procedures for an employee, and then what is out of non disclosure agreement this employee should do, and how do you keep on educating this employees on this.

So, that is a very big roll the HR as to play. So, so to some up this slide, what we have done here is that when we are looking at an information security policy, and the subsequent standards and procedures, we need to clearly identify these internal people and the external people, and also make the HR policy very strong. I have seen in many organizations, where there core business is not information technology. For example, banks, the core business is banking not information technology. They treat the information technology division of the bank, and also the main employees of the bank at the same level, from a HR perspective. I think in my opinion, in my very humble opinion it is wrong. There should a different hr policy for the information technology division of any organization. Be it a factory, a car factory there be an IT division there. The HR policy for the normal factory should be different from the HR policy of the IT factory. the education that this going to be imparted there, the type of roles they are going to be assigned, because they essentially over a period of a time or already would be the backbone of the entire organization.

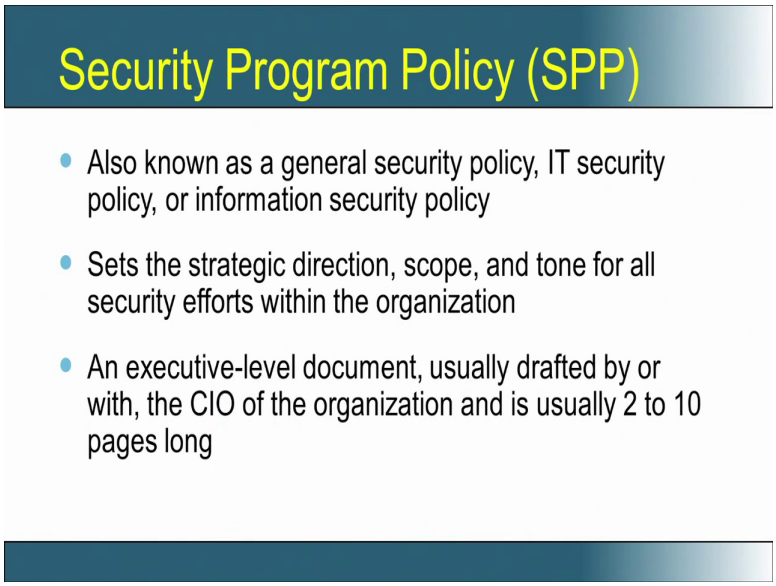
It is not just they should given is special treatment, but it should be given at different treatment there; the type of discloser agreements that you get sign, the type of training you put, the type of trust that you need to build in them the, type of ethics that they need be educated upon if they do not have, that way you recruit right. There is a very big debate, we will we will talk about it in one face of this information security course, probably levels four or level five. Where you are going to look at psychological, and attitude type of analysis on how we recruit people for such type of information security business, that is very important. So, we have to look at it. It is more a social problem that we have already talked about.

(Refer Slide Time: 05:15)



Now, with this roles and responsibilities, let us basically look at the type of policies that will go inside a policy document. So, we are now come to a stage; we have look at a base line, we have looked at information classification, we looked at some roles and responsibilities. Now, we have an idea of what we need to achieve, but then now we need to have a very clear way of going and achieving what we have in mind. Please understand that between mind and the document, there will be a lot of differences, there will be lot of ambiguities that are introduced right. So, let us now look at, what will be inside a policy document. So, what are the different types of policies that you can see, you could have a general or security program policy. We could have policies for specific issues. So, we call it as issue specific policies, security policies. We could have security policies which are specific to systems. So, we could have systems specific security policies. So, three different policies come into your information security policy document; the general or security program policy, the issues specific or security, insure specific security policies, the systems specific security policies.

(Refer Slide Time: 06:48)

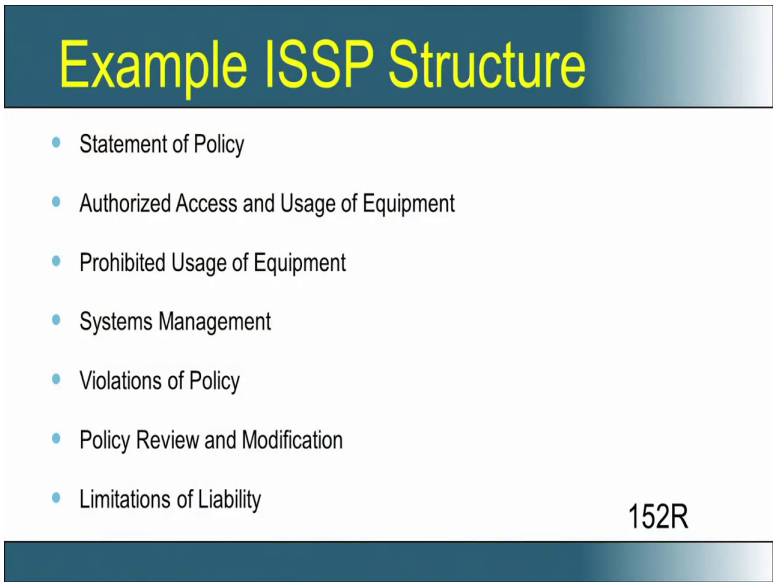


Now, we will go and look at this in greater details. Now, what is a security program policy. This is the sixty thousand feet abstract level of here information security. So, this is generally called your IT security policy, or the information security policy which your board sees. It will be something two to ten pages long. It is a very executive level document, usually drafted by the chief information officer of your organization. This will talk about strategies for security; this will talk about broad guidelines of security. I am not talking about policy with. The policy itself says should give you broad guide lines and the standard document should take, should be driven by this policies. But even with in this policies you will have at least three different type of policies; the first one is the security program policy, which talks about very broad guide lines.

(Refer Slide Time: 07:48)

Now, the next type of policy you will see inside a security policy document, is the issues specific policy. What is this issue specific policies? It talks about the technologies and the process that are needed to support certain routine operations. It will address specific areas of technology, and it is also important that we may have several independent issue specific policy documents; one for network, network policies, another for backup, another for third party. How do you we identify a third party, what are the basic think, so there should be a policy. So, these are all issues specific policies inside an information security policy document. So, though this looks very obvious I go back to my first statement of Bertrand Russell, obviousness the enemy of correctnesswe should be extremely careful in making this policies, for a simple thing is, that we try to make these policies modular. Modular in the sense that, there will some very generic things. Suppose I am looking at a technology say backup. There should be some generic statements about backup. Then there should be something specific about current day backup. So, when I want to revise these policies, because issues keep changing, technology changes, processes is changes, people changes, aptitude changes, so the policies also have to change. So, when this issues specific policies change, I need not go and change the entire document, when I have a modular approach. Some part of the document remains the same, and some part which is very much closely coupled to the issue alone changes. So, this is all about what we need to have at a very high level, and understanding of issues specific security policies.

(Refer Slide Time: 09:57)

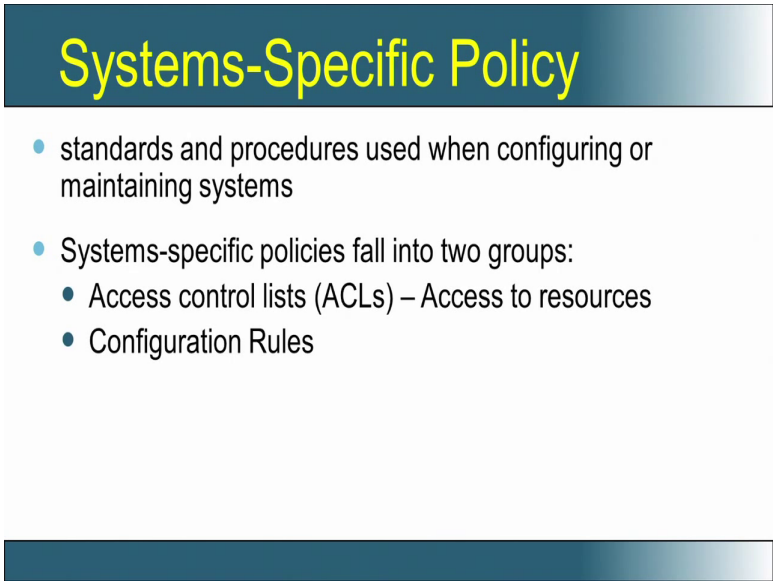


Now, let us go and very clearly look into the structure of this issues specific security policy. First and foremost there will be the statement of policy. I want you to concentrate on the slide. There will be a statement of policy. What do you mean by the statement of policy ? The policy should begin with a clear statement of purpose, and there should be a introductory section that should outline the scope, and applicability of the policy. And what is this policy actually address ? It will say who is responsible and the accountable for some of these policy implementations. What technologies and issues does the policy document address? It actually addresses about authorized access and usage of equipment. Who is authorized access which part of your asset ? This section of policy statement addresses, who can use the technology governed by the policy, and what it can be used for. And it also defines fair and responsible use of equipment and other organizational assets. And should also address key legal issues; such as protection of personal information and privacy.

The other thing this ISSP looks at, is also the prohibited usage of equipment. While the policy section describe above detail what the use of technology can be used for. This section also outlines what it cannot be used for. So, unless said organization says you are prohibited to use this equipment, it cannot enforce a policy there. So, when I say, x is allowed to use this equipment, you should say who are all those not x who cannot use this equipment. So, that should also be part of your ISSP structure. Then this policy also talks about systems management. And when you talk about systems management, there could be several information security related policies, and they all merge with each other,

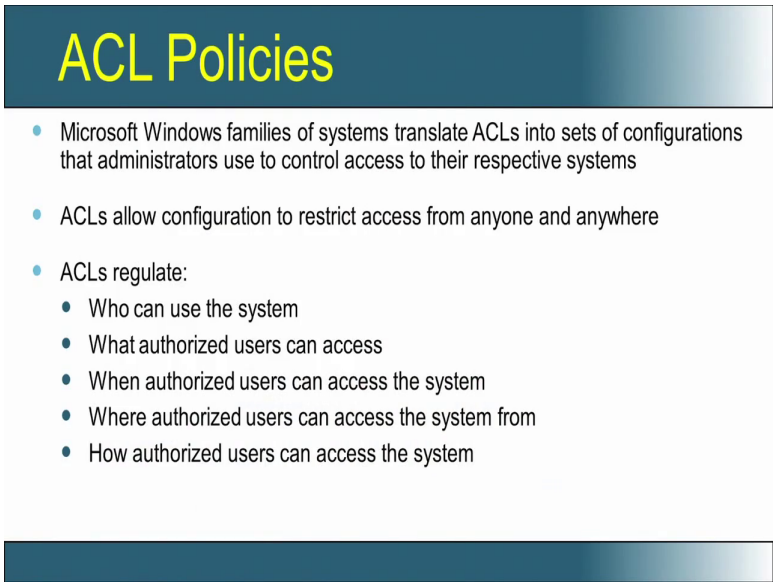
and there could be several issues that are common on different parts of a system. So, there could be some violations of policy. I determine a policy for one issue and that could go and hit another issue. So, these types of things could also be there. And the ISSP structure also will talk about how do you review this policies, and how do you modify this policies. And it should also talk. It should also come out with an analysis of, what are the liabilities of these policies, and what are the limitations of liability, more important. So, it should come out it disclaimer which essentially says, ok this is what I can do, and this is what this policies is about, and this cannot go and talk anything more than that. So, an issues specific security policy, for every issue you will have some policies, and these policies there will be several such security policy documents, and each of these policy documents will have all the seven points that I have stated here.

(Refer Slide Time: 13:29)



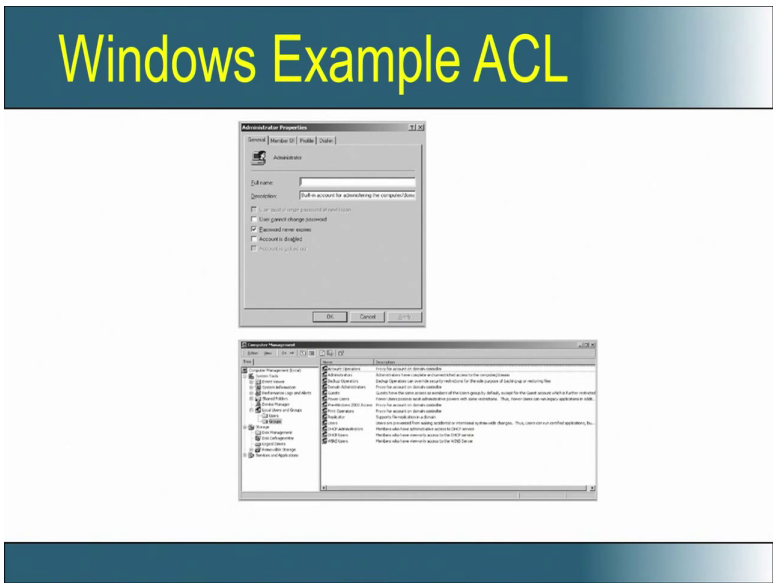
Now, we will go to the next one, which is the systems specific policy. These are basically standards and procedures used, for configuring or maintaining the system. So, system specific policies can be of two types one is the access control list another is a configuration rules. What is the access control list essentially mean ? It determines which the access to resources, who can access which resource. The manifestation of this access control list is again another configuration, which will go and configure who can. So, it will configure the resources in such way that, some people have access to some resources, and some do not have access to some resources. So, let us look at this in a more. ACL policies micro soft windows are very famous for theses type of ACLS.

(Refer Slide Time: 14:24)



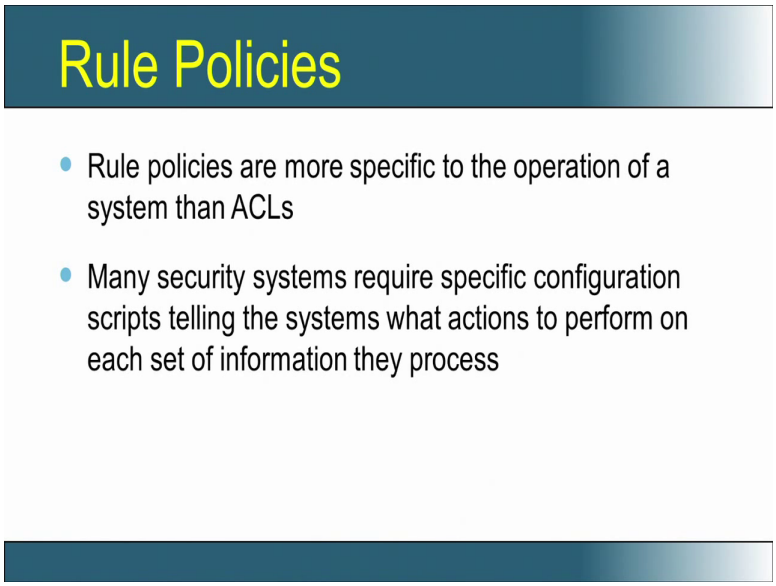
They actually translate this ACLS into sets of configurations. So, ACLS regulates, we have been talking about, but let me keep repeating that ACLS regulate, who can use the system, what authorized users can access, when authorized user can access the system, where authorized users can access the system from, and how authorized users can access the system. Each one of them is a very different question. So, when you look at implementing an access control policy. You need to answer these five questions.

(Refer Slide Time: 15:01)



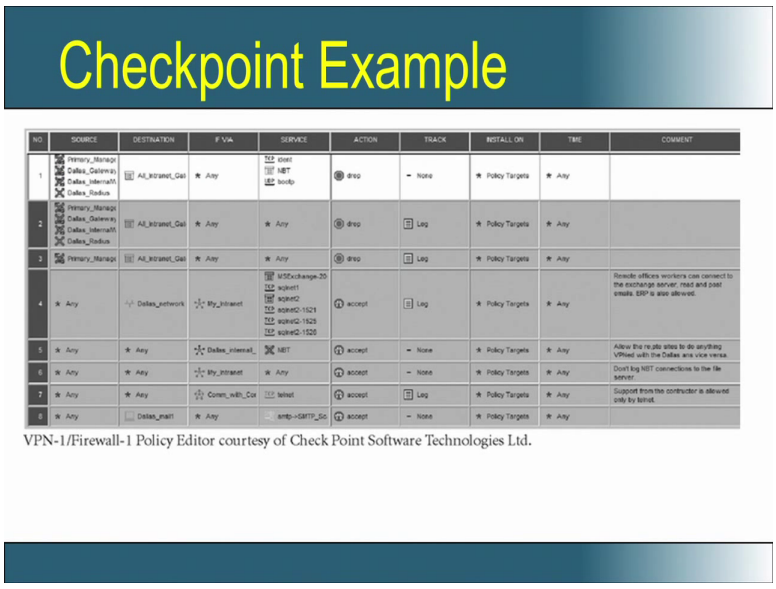
Now, the ACL policy; suppose to say we are using their windows operating system. We can see on this screen, the ACL policy set some role for an administrator. He says you can use only this.

(Refer Slide Time: 15:17)



Now, we will go more onto rule policies. So, the ACL actually implemented a rule, but the rule policies can also be more specific to the operation of a system. Let us look at some of the rule policies.

(Refer Slide Time: 15:37)

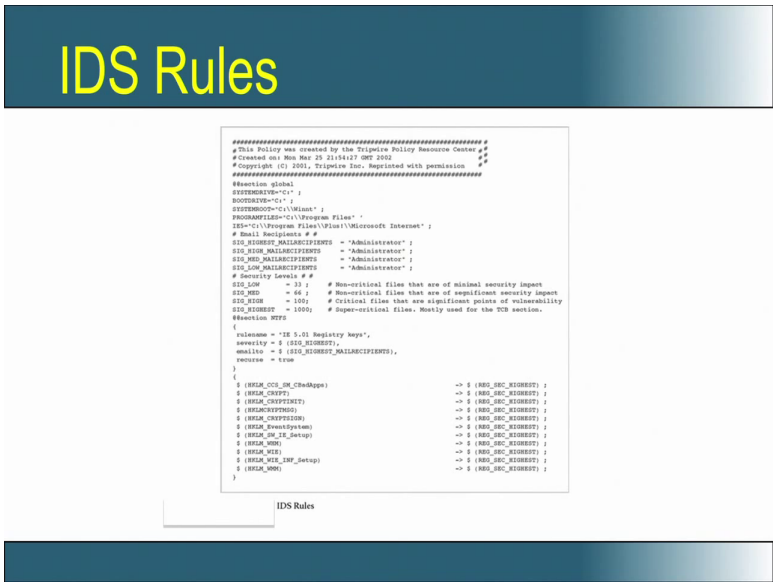


For example, let us look at this check point example. The checkpoint is basically for a firewall. What does this say? If the source of a packet, is in the first column. There are say now you see there are some eight rules. If there source is from some particular place it can also be any, and the destination is such some place, and this is originated by somebody, and this is the service, this is the action that you take, and this action should be tracked in such a form. So, this is a very interesting example of a rule or a

configuration. So, what I mean by a configuring a firewall. A firewall basically or virtual private network basically says, that this is what you need to do, when we do for different things. So, if my source is a and this destination is b, then I need to go and do something in that range. So, this is what we see in this. One interesting thing that we could also see some where you see drop correct. So, in the first and second line. What does the drop mean ? The drop essentially means, and some where you see accept. So, if you get from this source, and addressed for this destination drop the packet. I do not want that source to access this destination right. So, this is what you do in a firewall.

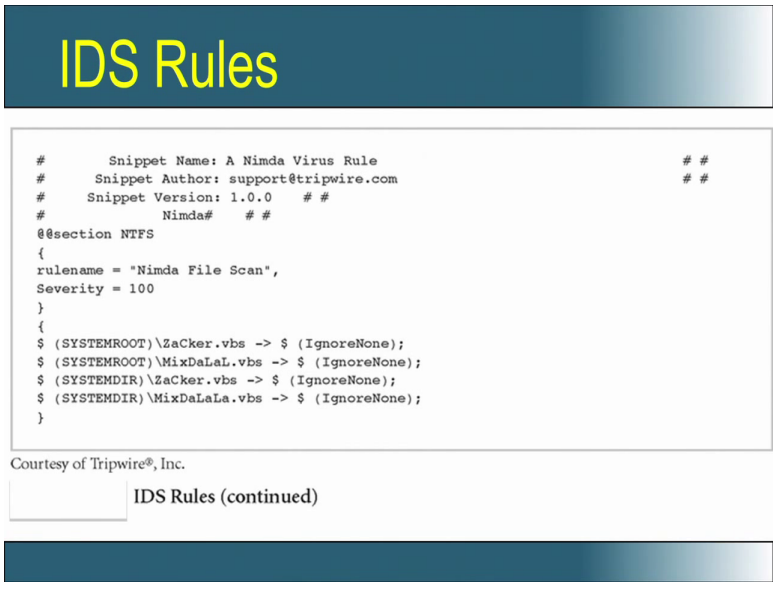
Though we are put in a very simple screen, the actual firewall if you purchase it is so costly. Now, I leave it your imagination of why this is costly, in some module down the line even within this course we will talk about firewalls, how difficult it is stay wall firewall. Now, you can actually go. See one of the important goals of this course, specifically from a management perspective, if you are in the information technology management, is that you understand some these functionalities, and then we leave it to your imagination to do prize discovery. Somebody comes and says this product is say hundred thousand dollars. Now, you should know what is inside that product, then it will be easy for you to do a price discovery. So, one of the very important goal of this course, is to educate you on price discovery. Now, at least you understand one is the functionality of a firewall. This is very simple as it says, but then how difficult it is to implement. Again security policies are easy to mention, but very difficult implement. I repeat this statement again. We will go and deal about firewalls and networking in module four in more detail.

(Refer Slide Time: 18:31)



Now, there is another intrusion detection systems IDS. There are some rules. As we see these rules basically tell you if there is this type of an intrusion.

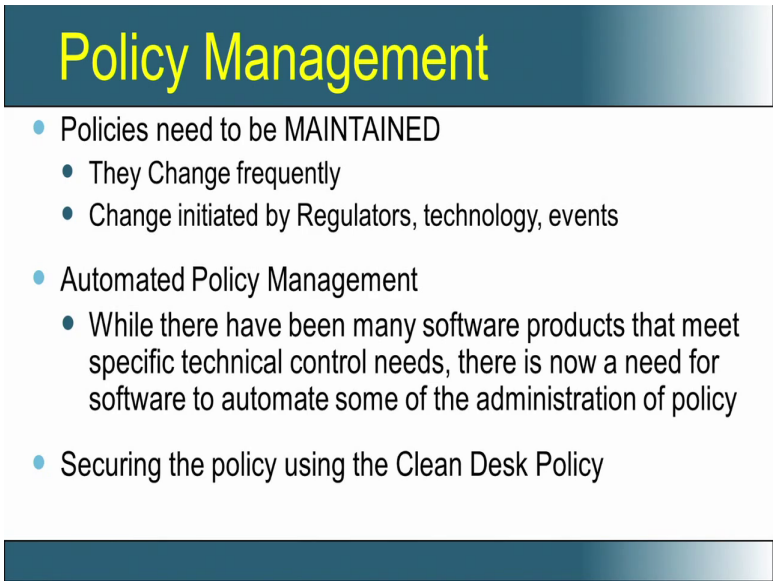
(Refer Slide Time: 18:43)



Let us go to the next slide where you actually see this type of an intrusion comes, then this is the action you take. If this in type of intrusion comes, do not take these actions. So, so this is again, you have a system, you have a network, and basically your data packets are coming, you to a big analysis on these packets. This is called deep packet inspection. You do lot of analysis on the packet. When you talked of the firewall, it does analysis of the header of a packet. What is an header ? Header basically says, this is the source, this is the destination, but when you talk of intrusion detection, you actually go

deep into the packet and find out if some patterns exist. And if those patterns exist, now go and do certain actions, and that is what essentially intrusion detections systems says. I am slowly trying to educate you on what is the difference between a firewall, and a intrusion detections systems. And as when some case studies like this come, I will take this opportunity to talk about different technology. But nevertheless from this particular module point of view, we have understood what do you mean by configuring a system. I have given an example of configuring a system through these, that the firewall and the ids.

(Refer Slide Time: 20:09)



Now, in the next session we will talk about managing policies.