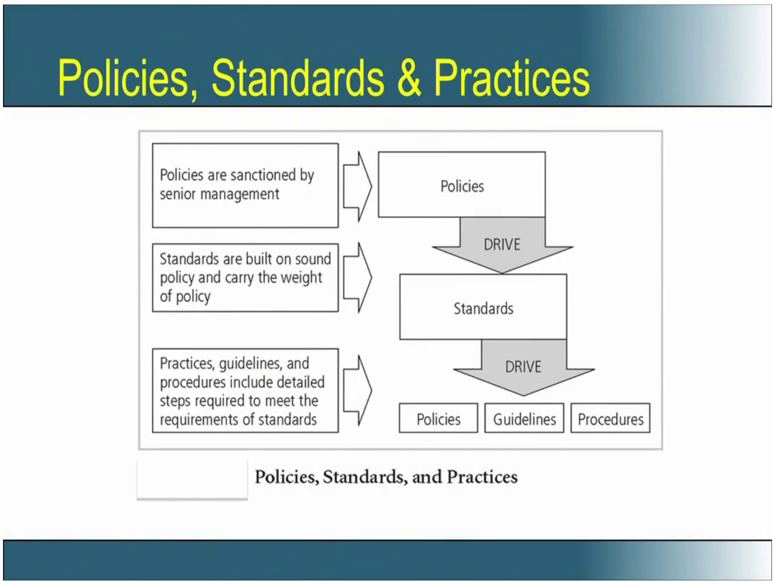
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 14

Now, we shall talk about the three important documents that form the information security documentation of in organization. There need to be a information security policy. There need to be an information security standard. There should be an information security practice. Three documents actually comprise the information security, documentation of an organization. Now, we should clearly understand; what is a policy, what is a standard, and what is a practice.

(Refer Slide Time: 00:43)



Policies, Standards & Practices

Policies are sanctioned by senior management

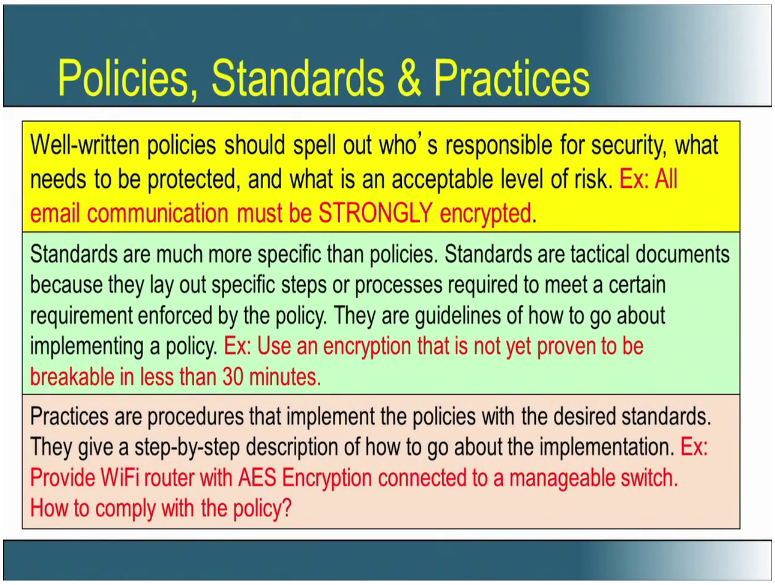
Standards are built on sound policy and carry the weight of policy

Practices, guidelines, and procedures include detailed steps required to meet the requirements of standards

Policies, Standards, and Practices

As we see in the slide; the policy are sanctioned by senior management that drives standards, which are build on sound policies and carry the weight of the policy. And these standards actually drive the guidelines, which are basically practices, and procedures that include details steps, required to meet the requirement of the standards. This is very easily defined, but very difficult to comprehend. So, let me start giving examples, where you clearly understand the difference between a policy, a standard and a practice.

(Refer Slide Time: 01:24)



Policies, Standards & Practices

Well-written policies should spell out who's responsible for security, what needs to be protected, and what is an acceptable level of risk. Ex: All email communication must be STRONGLY encrypted.

Standards are much more specific than policies. Standards are tactical documents because they lay out specific steps or processes required to meet a certain requirement enforced by the policy. They are guidelines of how to go about implementing a policy. Ex: Use an encryption that is not yet proven to be breakable in less than 30 minutes.

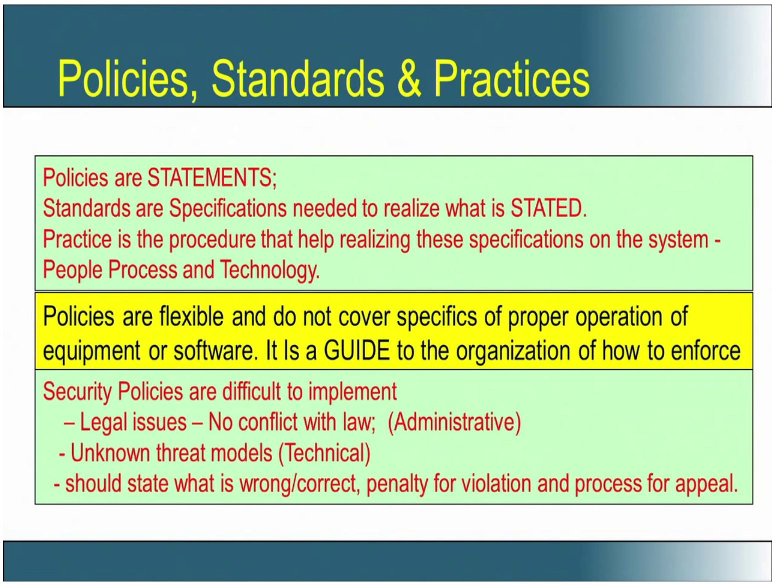
Practices are procedures that implement the policies with the desired standards. They give a step-by-step description of how to go about the implementation. Ex: Provide WiFi router with AES Encryption connected to a manageable switch. How to comply with the policy?

So, well return policies should spell out, who is responsible for security, and what needs to be protected, and what is an acceptable level of risk, but you actually stop there. For example, all email communication must be strongly encrypted, this is a policy. And it will say who is responsible for ensuring this policy. There will be one part of the IT wing, or communication part of the IT wing, and they will say he is responsible for seeing that all email communications are strongly encrypted, and the policies stop here.

Now, when somebody evolves the standard for this policy, this policy will drive that the next document, the standard document to go and include statements like; use an encryption that is not yet proven to be breakable; say in less than thirty minutes, this is what the standard will say. So, what is driving this standard; the word is strongly encrypted derives the standard, this go and say that you cannot break it in less than thirty minutes. So, in general standards are much more specific plan, much more specific than the policies. They are basically tactical documents, that layout some specific steps and processes is that are need to be followed to achieve certain goals.

Now this standard will go and drive a practice. What is practice? Practice is that clear down to earth, step by step procedure by which you go, and implement a policy statement, with own desired standards. So, there is a policy, and there is a standard which it has driven. Now the procedure will go an implement what the policy says, as decide by the standard. For example, in this case provide wifi router with AES encryption, connected to a manageable switch. So, this will give you that AES encryption for example, can give you an encryption, which is less than thirty minutes, which ensures that within less than thirty minutes one cannot break a password. So, policy essentially talks about very broad guideline. The standard goes into a little more specific, and the practice actually implements this. So, what should be path, all that I have put in red in the slide, should be part of the different documents. For example the policy here with say, all email communication must be strongly encrypted. Your standard should say use an encryption that it is not and proven to be breakable in less than thirty minutes. And that third AER practice should say, provide wifi router with AES encryption connected to a manageable switch.

(Refer Slide Time: 04:31)



Policies, Standards & Practices

Policies are STATEMENTS;
Standards are Specifications needed to realize what is STATED.
Practice is the procedure that help realizing these specifications on the system - People Process and Technology.

Policies are flexible and do not cover specifics of proper operation of equipment or software. It Is a GUIDE to the organization of how to enforce

Security Policies are difficult to implement
– Legal issues – No conflict with law; (Administrative)
- Unknown threat models (Technical)
- should state what is wrong/correct, penalty for violation and process for appeal.

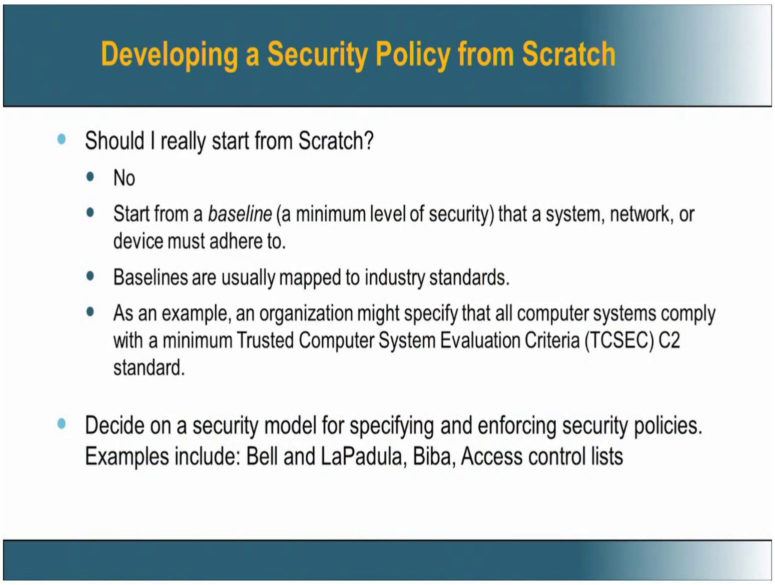
So, just elaborating on what you have seen. Policies or basically statements, while standards as specifications, needed to realize what is stated, while practice is the procedure that help realizing this specifications of the system. Policies should be flexible; otherwise you lose direction. For example, while arriving at a information security policy. Suppose I talk of AES, it is not what policies should say. Then it means that the fellow is implementing the standard, the fellow is realizing the fellow is arriving at the standard, and the fellow who is actually realizing it in practice, will lose all the flexibility. He cannot do in any cost benefit analysis. So, in some essence the policy should be very broad guideline, and it should be flexible. It should just be a guide to the organization. . So, when you are arriving at a policy, you start going to nitty-gritties, you also lose the focus, the main focus of the policy.

The main focus of the policy is, more than just giving all these things. We have to also look at another very important aspect; namely the legal issues. There should be no conflict with law, and this is a administrative aspect of the security policy. For example, I want to put camera's to monitors, then there is a law which says that you should explicitly state, that you are being monitored. I cannot actually make an encryption algorithm for my phone; a telephone which, and communicate voice with using personal encryption, on a normal phone. I may not, a countries' policy may not, different countries should have different policies. So, when I am doing encryption of voice call on a normal telephone network, even because when the telephone calls in main office and a branch, would be a normal telephone. So, can I go and encrypt. So, there can be some telecom regulations there. So, all these things need to be taken care, when you are arriving at a policy and a standard.

More importantly you do not know you threat models. How somebody is going to attack you, you do not know. So, we need to half lot more technically insight into this. So, the policy should basically dwell upon what is correct wrong, and if somebody does the something wrong what should be the penalty for violation, and if the person feels that he has not done something wrong, there should be an process for appeal. So, please understand that the whole environment that we are taking of today, is not a very well defined environment. For the simple reason that nobody understands, what are all that threats. So, I cannot just go and. So, we will have some broad guidelines, and we will have certainly some penalties for this broad guidelines, but then these guidelines has to constantly we refined based on experience. and again we should keep what law says, that "no innocent should be punished, hundred criminals can go unpunished, but not one innocent should be punished", that is very important; otherwise this will not give a security to the user.

So, when a user uses it, and if there is an unknown threat; at threat we he which he is which does in know happens. For example, suddenly some money from your account, from your costumers account goes off. The bank should not go and say you are wrong to the customer, then you will not using internet, you will not use any of your alternate channels. Then there will be regulations which will be say that, cheque books are mandatory. someone opts to keep out of alternate channels, should be given the permission to. There should be a way by which someone, can keep out of alternate channels; like your internet banking or mobile banking. Then there will be a regulation like that. So, if you really want people should adapt it, after they are convinced. And if there is some violation that has happened, there should be enough proof to go and prove that the violation as happened, because of a wrong doing of some individual. And that proof in today's context, is going to be a very complex thing, because somebody has hacked into your account, is it because you broadcasted your password, or he hacked into the password. it is because your password was weak, or it is because the software that was actually evaluating the strength of the password is weak. so many dimensions come into it. and so this is the basic difficulties, so that is why we say, security policies are easily said, easily lectured, but very difficult to implement.

(Refer Slide Time: 10:02)



Developing a Security Policy from Scratch

- Should I really start from Scratch?
  - No
  - Start from a *baseline* (a minimum level of security) that a system, network, or device must adhere to.
  - Baselines are usually mapped to industry standards.
  - As an example, an organization might specify that all computer systems comply with a minimum Trusted Computer System Evaluation Criteria (TCSEC) C2 standard.
- Decide on a security model for specifying and enforcing security policies. Examples include: Bell and LaPadula, Biba, Access control lists

Now let us go, and I just want to end this module from here to the end of these module. I want to basically talk about, give you a guideline on how you can implement a security policy from scratch. The question is, should I really start from the scratch. The answer is, no you cannot really start from the scratch. one of the important things that, at least I believe, is that all the security vulnerabilities, should be made that organization phases, should be actually made open, because it is a collective exercise for all of us to learn. The regulators also should encourage people to come out openly on the vulnerabilities they have faced. Yes there was a vulnerabilities, based on which, there was a fraud that as happened in this organization. This should not be taken as you know as a black mark on the organization, because the same vulnerabilities can happen to another organization at some point of time. So, there should be a collective learning that should come up.

So, that comes out with more strong security measures. The organizations, the management should also come out of this stigma, that if there was a vulnerability. There is indeed a big black mark on the organization; it is not a case, because nobody has actually understood the very large threat model. What are the different possible ways by which somebody can attack you system; that is not a very comprehensive model. given that I do not think anybody should feel very bad if some things happen, but nevertheless you should take lot of steps to prevent frauds, IT related frauds, but there should be a forum, where people should open up their mind, and talk about the real frauds that are happening, and that should be a collective learning. So, given this let us go. So, there are certain standards. For example, the trusted computer system evaluation criteria the TC 2 standard that is available. So, there are several standards which could be taken as a base line, for developing a security policy.

What is a base line, a minimum level of security that a system network or device must adhere to. This base line document is available. And you take this base line document and start building on top of it. And once you have its baseline document, then you can also have the theoretical models like a Bell and Lapadula; theoretical model well established and practiced today; bell and Lapadula model, the Biba model, the access control list etcetera, which will help you, build the security. We have talked about these models in the early part of module one, and we will talk about it in larger detail, in our subsequent information security introduction courses; level two and level three, which we plan in subsequent months.

(Refer Slide Time: 13:08)

Step 2: Information Classification

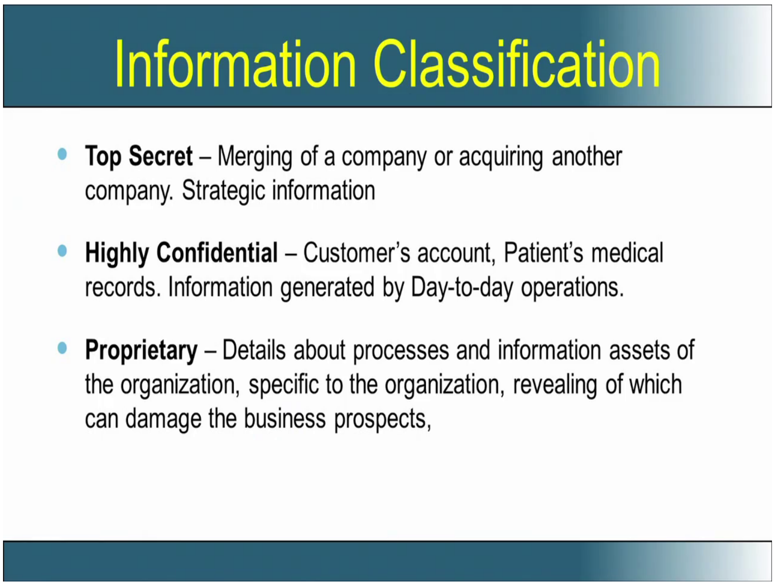
- Classification based on Sensitivity
- The classification should not be complex
  - Easy to comprehend
  - No duplication of classification.
  - If duplication occurs the higher of the sensitivity is used.

Once you have a framework, you decide on a framework, we have given you some examples and some models, some study. The next important thing is that, how do you classify your information assets. Naturally we are classifying your information assets based on the security, because you are talking about information security here. So, you basically classify it based on sensitivity, sensitivity of the information. But again this classification, should be easy to comprehend. You should not have a classification that people cannot even understand, because the person who is going to classify. For example, risk management; suppose I want to do a risk or risk management of different assets that you have, different accounts in a bank for example. When going to implement some crazy policies, the actually a manager when is trying to given a loan right. He has to understand and what is the risk involved, and your policy should helping understand. You cannot put some hundred thousand formulas and say, you go on work on this formula and evaluate, because this is lot of subjective evaluation needs to happen here.

So, when you classify information. we just given an example of this, your information classification should be very easy to comprehend. And there should be no duplication of classification, that is something. So, at some point when I look, this information is of priority or a level two of confidentiality. When I see from another angle it is level six of confidentiality, this type of inconsistency should not come. And in case this type of inconsistency is come when your classifying information, then we should say that if duplication occurs, the highest level of the sensitive so far should be assigned to that. So, even at some point the some way of looking at some information asset. If I say it is level six, but some other fellow, some other way of looking at the information asset some other procedure wants it to be level two, then this particular information asset will be at level two.

Now, this is the broad guideline of how do you classify information, but now we will come into specifics of information classification. Information can be top secret. See we should understand. So, everything cannot be top secret. So, what is top secret. So, I want to go and start discussing about merging my company with something else, some other organization. Or I am having very strategic information, I am going to prize this that some ways, so that I have a competition edge over other. I am trying to evolve a product for the next generation. So, these type of information are very top secret, and once it is leak the entire company or a business model, totally can collapse. Then there are certain information is needed to be kept highly confidential. For example, customer’s account, very difficult to get the amount of money, somebody stored in some bank, for x to get information about y, It is a highly confidential, or a patient’s medical record for example, if you look at information security at a health level. The HIPPA type of policies say. So, this is information generated by day to day operation. These are also highly confidential.

(Refer Slide Time: 16:48)



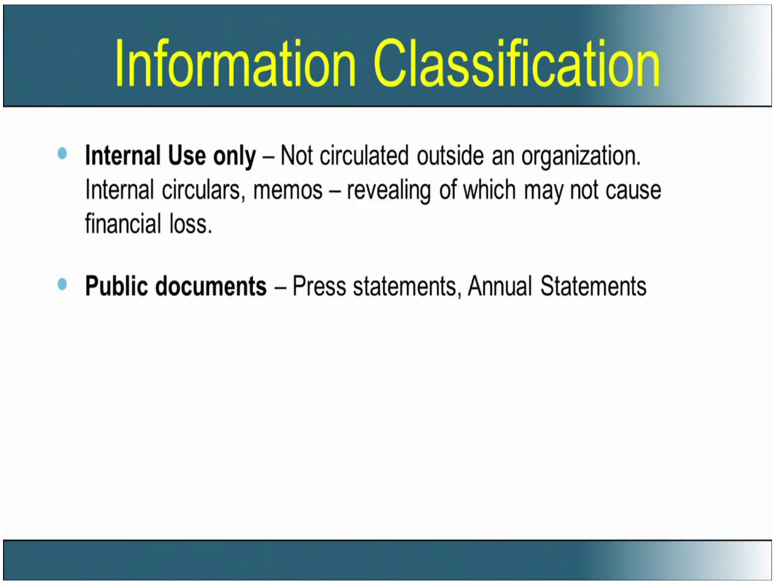
Information Classification

- **Top Secret** – Merging of a company or acquiring another company. Strategic information
- **Highly Confidential** – Customer's account, Patient's medical records. Information generated by Day-to-day operations.
- **Proprietary** – Details about processes and information assets of the organization, specific to the organization, revealing of which can damage the business prospects,

But some leakage of this, for example, profit and loss on a particular quarter, is highly confidential, is not top secret. So, what it is highly confidential, because once you leak it, it may have some temporary or a semi permanent; say for a temporary, or a little longer duration impact on your business. It can have an impact, but it is not that your entire company will close. So, that is what we term as highly confidential. Then the next thing is proprietary information. This proprietary will be known to a larger section of your organization. For example, you have already made a design, and that is going inside your product. it is not still that your revealed. For example, if I am going to merge a company a with company b I may not even revealed it to the second level management.

It is between CEO and the board or something like that, but a proprietary information is, I made a design and I am selling product, so out of this design, but the secret which is there in that selling of this product should not be leaked. If it is leaked, then it becomes very big your competitiveness in the market. Somebody can really istart mimicking you. So, that is why the intellectual property rights, IP patenting and other things come of this, but the details about some of the processes is, and some of these things that are very specific to your organization are called proprietary information, and that should not we revealed. So, there are clauses the employees actually sign, what you call as the non discloser agreement, basically for these type of proprietary information, but please understand that the three information that I have put in the slide or indeed different..

(Refer Slide Time: 18:40)

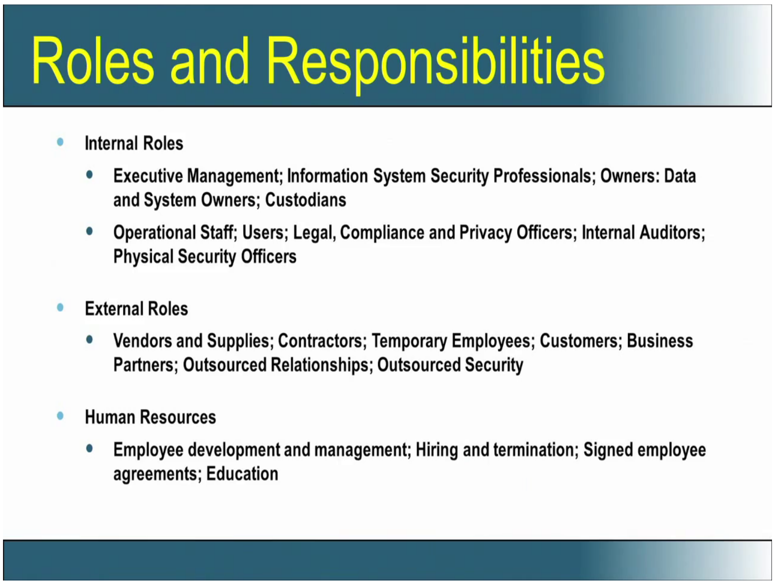


Information Classification

- **Internal Use only** – Not circulated outside an organization. Internal circulars, memos – revealing of which may not cause financial loss.
- **Public documents** – Press statements, Annual Statements

Then there are information which are only internal use only; for example, the memos given, or internal circulars, or revealing of, which may not cost financial loss or which may cost financial loss. These are all circular switcher internal to the organization, which should not be revealed to the external, but here more people come to known. Then there are public documents; which are press statement and annual statement extra. So, when you look at the classification of your information assets.

(Refer Slide Time: 19:42)



Roles and Responsibilities

- Internal Roles
  - Executive Management; Information System Security Professionals; Owners: Data and System Owners; Custodians
  - Operational Staff; Users; Legal, Compliance and Privacy Officers; Internal Auditors; Physical Security Officers
- External Roles
  - Vendors and Supplies; Contractors; Temporary Employees; Customers; Business Partners; Outsourced Relationships; Outsourced Security
- Human Resources
  - Employee development and management; Hiring and termination; Signed employee agreements; Education

Now we are talking about document alone. We have been talking about document alone; the same thing is for the software, the data etcetra. We have also talked about data for example, the patients data and customers account information extra. So, if you look at, from the top secret, to highly confidential to proprietary, to internal use to public documents. The number of people who will have access to this information increases from top to bottom, it is like a pyramid. Now in the next, we will talk about roles and responsibilities.