Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 05
Lecture: 14

And to understand related concepts, concepts that are related to policy. For example, there is policy and then there is procedure. And policy and procedure are different. So that is what this slide illustrates, policy, standards, procedures and guidelines. I would say standards and procedures are the next level of policy. Policy is broader.

Policy is abstract. Policy relates to the strategic purpose of the organization and also ensures that the organization achieves its objectives without compromising on law and freedom of individuals etc. So, it is a very broader philosophical level statement, where, in standards actually provide you more details of how the policy would be enacted or implemented. It is the next level.

And it will always refer to the policy. It will can be very strict on cyber security. It can be moderately strict, based on how the policy is formed. I can give an example. Today, we will be uploading certain policies of, cyber security policies of certain organization from different domains on your module.

We do not have time to present different policies, but refer to those documents. It will give you a picture of how policies are different, say in healthcare and education. The priorities would be very different. So, that also depends on the sensitivity of information and data that needs to be protected. But in India, I can say the cyber security policy of an academic institution may not be as strict as that of a healthcare organization.

But if you go to the West, say I showed you the document related to Carnegie Mellon yesterday, how detailed it is, because privacy concerns differ across cultures and countries. And therefore, the law is also different. So therefore, it may get stricter in future in all domains, but it differs across domains. Standards are the next level of documents. I deviated a bit.

And procedures and guidelines are documents that implement the standards, drawn from policies. And as we saw previously, policy is a document that needs to be implemented at the end, as management guidelines and technical implementations. So at the granular level, if you say that the employees should be able to access legitimate sites, but they should not be accessing sites which are prohibited by law, that is a policy statement. Now

at the procedural level, firewall configuration rules. That is a procedure.

How your firewall is configured. That is the technical procedure. So you can see policy has laid down importance on some aspects. The procedure becomes something that implements that particular aspect of policy. So that is how you differentiate between policy standards, procedures and guidelines.

And it also requires that policy is disseminated or policy is communicated to the employees of the organization. Policy is not something that you frame and keep in a master document in the corporate office. And employees have no clue about it. That is not policy. Policy documents should be disseminated or policy should be made known to the individuals.

And you know, so when you join any organization, of course you read, you get a document on the code of conduct. Some organizations do, some organizations do not do. If you join a TATA, any TATA company, there is something called TATA code of conduct, which is framed by TATAs and organizations, you know, in the beginning. So if you join TCS for example, there is a code of conduct. And it is mandatory for you to actually know, what is the code of conduct.

But in certain other organizations, there is no such document as code of conduct which is drawn from the policy. Let me not mention which are those organizations, but it can happen. So policy dissemination is the responsibility of the top management. And particularly in the domain of cyber security, there is something known as SETA, S E T A. S E T A stands for Security Education Training and Awareness.

You may come across this terminology in cyber security related documents. SETA is Security Education Training and Awareness. What you are going through now is the E, Security Education. It is a full course that you are doing on cyber security. You are learning fundamental concepts.

You are going through certain theoretical concepts, I would say. But we see what you learn in the course is much more than how to do things, which is what training does. So it immediately prepares you, prepares you for certain practice. But there should also be long term education imparted on people, especially employees and also awareness. So that is where the drills, the mock-ups and so many things periodically is done to make people aware, particularly about new developments.

So if you are in an organization and if there is no security awareness programs, you and if you have a lot of cyber assets and if you are in a particularly in a new organization, like

the iPremier, keep in mind it is your responsibility also to ask for it. What are the cyber assets we have and what are the policies here and do we know everything. There should be periodic training and awareness programs initiated by the organization. If not, at some point you may also be running for your job. Because in a place where there is no clear policy and practice of cyber security when things go wrong, you know, it can shake up the whole organization.

So I think we are going to the next level in understanding what is policy, what is standard and what are cyber security practices, which is the implementation aspect. So policy, by nature is a long term document. You do not change a policy every day. It is not an operational document.

It is not a procedure. It is a reference document. It is a master document and it should not be changing frequently. There are other documents that can change. For example, if you, if some aspect of regulation is updated, for example, if our personal data protection act becomes a law and it suggests that a cyber incident should be reported within 24 hours.

GDPR says it is 72 hours. It changes to 24 hours. You do not have to change the policy. You have to change, well, the standard related to compliance. Because policy will say, state that the organization should comply with the law of the land.

It is a broad statement. How you comply, is a specific detail which will come in the standard and procedures. So therefore what I am saying is, compliance to law is insisted in the policy. That does not have to change. Details can change, in terms of the subsequent documents. Now policy is having three dimensions or I would say it is a, you can see it as a hierarchy.

The first, the top document is the Enterprise Information Security Program Policy known as EISP. Now the second level is the Issue Specific Information Security Policies known as ISSP. And System Specific Information Security Policy or SysSP is the last level. At a higher level, at the enterprise level, the organization says employees will be provided electronic mail communication facility. And it should be used in accordance, with the procedures and guidelines.

That is a policy statement. At the next level, at the issue specific information security policies there should be a detailed policy on email, email use. What are the policies at the next level, pertaining to the issue of email communication ? For example, how much storage space you get. And what kind of emails you can send and receive in a, in a organizational email account. Generally you are not supposed to use it for personal communications. It is for professional communication.

So these are actually guidelines that comes at the issue level, the next level. And the third level is System Specific Information Security Policies. This is the implementation stage. The institute says you can have up till 5 GB storage. Well, at the time of configuration, the server it will be configured as 5 GB and you cannot exceed 5 GB.

That is the third level of issue, system specific information security policies which becomes the rules, which are configured technically and for which guidelines are given. So policy operates at three levels, at the enterprise level which is the highest level, which is related to the organization strategy, mission and vision. Issue specific is about, you know, it takes into account the various technologies that the organization has and issues related to that. So the second can also be called the technology philosophy of the organization. It could be about electronic communications, it could be about, it could be about file storage, it could be about cloud, it could be about various other aspects of technology that the organization uses.

So it is at the technology level. And third is it at the configuration level. So this is a broad purview of policy. Now I have already explained this. So EISP or Enterprise Information Security Policy or EISP sets strategic direction, scope, tone, tone is also important, the choice of words. How important something is, how light something is, depends on the choice of words.

Most important or critical, you know, if you use those words, you have to keep in mind that well, it is a very critical thing. Or if somebody says our organization gives due importance, that is a bit subject to interpretation, what is due? It is a bit subjective and that is where actually you bring in words and English vocabulary is so wide. So you can actually choose words in such a way that it communicates what is the priority that you gave to certain areas and what is the less priority possibly you may give to certain other areas. And you have already seen that if you give top priority to something, you are committing resources, you are committing money, you are willing to pay the cost that is required to implement it. Assigns responsibilities for various areas of information security and guides development, implementation and management requirements for information security program.

So policy is a document, but policy is also a plan or it is a basis to plan the subsequent activities, choice of technologies and implementation of technologies. So if you ask the question, what is the TOC, Table of Content of a EISP, broadly it will have the sections - statement of purpose. What is your purpose? When you read a policy probably this is the first thing come, what are you trying to achieve through this? And that is what is connected to the objective of the organization. And what do you mean by information

security? Are you covering only data information or is it a broader level like cyber security? What is in scope? Does it involve people or it is only about databases? So you have to actually make the inclusion, exclusion statement very clearly in terms of definitions because it is a reference document. You will see that detailed definitions of terms in the EISP because that is where you clearly say, what do you mean and what is the scope etc.

And of course, need for cyber security as to why this due attention is paid and who, what are the roles related to it? For example, do you have a CISP, Chief Information Security Officer, CISO, sorry. Is there a post of CISO? Keep in mind hiring a CISO is a, it is a costly position, there is salary involved. So hiring such expertise is a cost to the organization and then there should be a subsequent organization, a sub organization. So that is a investment in people resources. Is the company committed to that? If not, you do not mention that in the policy document.

You may look at the, you may search for a policy document of IIT Madras. Is there a CISO job or not? Possibly you will not find, at the moment. We have not realized the need for it. But go to Apollo Tyres, sorry Apollo hospitals and see what is the cyber security structure they have. They have a CIO, CISO, they have everything which is required to professionally manage the cyber security of that organization.

Refer to some of the policy documents which we are going to upload. You will find this. And reference information technology standards and guidelines. For example, if you are going to follow an NIST or ISO standard, then you can actually give a reference to that in the EISP, but not the details. Then comes the next level, which is the issue specific security policy or ISSP.

Keep in mind EISP, ISSP, SysSP. SP standing for security policy. These are standard terminologies, conceptually standard terminologies. A textbook for example or research papers may all use these terms. But there could be variations in terms of these roles and their labeling in organizations. So, somebody may call the top person in cyber security, a Director - Cyber Security.

Somebody is not well informed for example, but you need someone to head this. They have not gone through security training. The top management has not got cyber security training. So they may give more other terms.

So there is Director - IT, in several organizations. So that may not be the right thing, which is generally accepted. It is a CIO. So you may, my point is, these documents may be titled differently, but in a more generic sense or conceptually correct sense, it is the

next level of cyber security policy is the issue specific security policy, which provides detailed targeted guidance to instruct organization, to secure use of technology systems. So as I said, ISSP is the technology level. EISP is more into the organization and the cyber assets.

Here you do not refer to the organizational priorities etc, in the ISSP. Well, email use or cloud use etc. It refers to technologies and lay down clear guidance on the use of technologies. That is what issue specific cyber security is. And also it gives guidance on how these systems are controlled, monitored etc.

For example, malware detection and if there is an, if somebody accesses a site which is not legal, the firewall can actually detect that and it can also detect from which machine the accesses happened etc. So there is monitoring involved, which the employee should know in a document. And the third aspect is what I have highlighted. It serves to indemnify the organization against liability.

So Indemnification is a legal term. Are you familiar with this term "Indemnify"? What do you mean by indemnification? Protect yourself from what? Indemnify would mean to absolve someone of the responsibility - absolve someone of responsibility. So, do you think in an IT industry, in an IT organization, should the organization indemnify employees by policy? For example, if someone makes illegal access to a site, should the employee be indemnified? Depends on the intention. Okay. Intention of whom? The employee. Can you elaborate that? But what intention would be right and what would be wrong? Intention actually, with what intention he was trying to do that.

Okay. Whether that was wrong or in the right sense. Okay. Part of the duty. I can give an example, you validated. Suppose an employee accesses a illegal site, by mistake. For example, there is a spam mail, where you get a lot of junk and out of curiosity you just clicked on something and it took you to a site which is illegal. It is actually a, it is not by intention that employee went there, but it is by mistake.

But of course, there should be evidence for that, but you can always. So in such cases an employee should be indemnified. Like it also depends whether that was a normal negligence or a gross negligence because now gross negligence will obviously. Yeah, yeah. That is something which is repeatedly happening or it is a standalone incident.

Yeah, so there can be events where employees need to be protected. But here it is talking about indemnifying the organization. The policy should be such that it protects the organization. Tomorrow, an employee does something wrong and the court should not be drawn to the court.

The employee should defend oneself. That is actually a problem, sometimes. See in certain professions, IT we can actually debate because it is employee's fault and so on. But in certain professions, if an employee is not indemnified, people will not go for that job. Because there can be more frequent legal issues in certain professions. And certain professions by nature, you may take risk and do certain things.

A good example is the medical profession. In medical profession, doctors treat patients and the patient's status would be very different. Some have come with prior serious medical problems and the doctors sometimes have to try out different medicines because something is not working. Of course, they take consent of relatives before doing such critical things. But in certain cases, despite in normal course of treatment also, it may not be doctor's negligence but patients can actually respond and die. And see in such cases, if the doctor has to go to court, then the profession becomes very uninteresting.

So that is why in medical practice, the doctors are indemnified. It is the hospital that fights for the cases. So indemnification from such consequences is important for employees, not for organizations in such cases. The healthcare system protects its doctors. But in certain other cases, the organization would indemnify itself.

That is what we see here. Because the patients, sorry, it is not the patients but the employees can actually misuse or abuse resources and that is the more likely thing to happen. So issue specific security policy also have indemnifying clauses. That is where it helps you in the legal fight, often times. So examples of ISSP issues and topics here for you to develop better understanding. It is a statement on the organization's position on an issue and the issues and topics could be like the emails, worldwide web, the policy on worms and viruses, hacking, testing of organization on security, to what extent you can go and you should not go.

And now a policy that is still evolving is work from home. Post pandemic, there is the work from home arrangement and also bring your own device. Using your own devices, sitting at your home, you will be accessing the resources of the organization. And generally it is reported that, when employee is not in the, within the walls of the organization, when you are the there is, when you are elsewhere in your own place of comfort, there is some sort of absence of a perception of a guardian, you know, the place of work serves as a sort of there is some guardian out there, somebody is watching, you know. So in the absence of that, the likelihood of commission of non-compliance is potentially high.

So these policies are still evolving. So one is you have to allow work from home, bring

your own device. At the same time, it should not work against the interest of the organization. So this is actually a policy situation, policy reframing situation. So components of the ISSP again, there will be statement of purpose. And as I said, this will be more based on different technologies, different issues.

It gets into that details, for example, prohibited use, systems of management, monitoring, physical security, encryption, all these will be detailed in the ISSP. Issue specific systems, sorry, issue specific security policy, violations of policy, policy review and modification and limitations of liability, indemnification, etc. So it is a very detailed legal document because this is also a document that you use, to defend the organization in case of violations. And the third is the stage, when you come to the implementation stage.

And that is known as system specific policy. Policy should be stated, policy education should be given or should be disseminated and policy should also be implemented. Or you have to create enabling situations. You cannot tell in the court that we have stated in the policy clearly that an employee should not do this or do that or access this or access that, but your firewall is allowing everything to go in. That actually becomes problematic.

So therefore, there should be two aspects to SysSP. One is the management guidance, other is the technical specification. Management guidance is like a procedure document. How you configure your firewall ? For example, that is a guidance document or a procedural document. And what is the configuration document actually, that is the physical or technical configuration. And management guidance document basically is generated to ensure the CIA, confidentiality, integrity and availability within the purview of the policy and law.

And for example, who accesses. So there is something called access control list or ACL, which is implemented at the technical level in computers, say in Windows or in your iOS machines, the access control list is something that is configured. So different levels of access and privileges. So the technical specs basically operates in two levels, broadly as ACL or access control list and configuration rules. I will just give you some screenshots as examples of this because this is the detail of technical spec. So access control list is nothing, but certain roles and what documents that role can access.

So it is a detailed mapping of roles and access privileges. For example, who can access a particular file. So there is a file which falls into a particular category and then each user belongs to a particular category. So that category mapping on, between resources and people is the ACL broadly. ACL actually in detail lays down who can access the system, what otherwise the users can access.

So we discussed this earlier when we discussed CIA. When they can access , you can set timelines also. When access is prohibited. For example, in some institutions you cannot access internet in the night. And in IIT there is no restriction, I believe. Where otherwise users can access the system, is it from the organization or outside, whether it is a LAN or open anywhere.

How the access can be done and so, for example, biometric versus password access as a simple example and what are those resources. And what are the access privileges, can you read only or can you write, can you create, for example, can you create a new table in a database or can you just write a query, modify, delete, compare, copy etc. So this is all part of the ACL and ACL is very detailed in terms of its implementation. This is the windows XP ACLs, just as a small example. On the left side you see different roles, from administrators to backup operators, guest network configuration group, power users and so on and what are their privileges.

Configuration rules - One is the ACL, other is the configuration rule. Configuration rules actually finally implements the rules, that are stipulated in the ISSP and in the management guidance that we have seen. Here is an example. The firewall configuration rule. Simple thing, which are the sites which can access the internal resources of IIT Madras that is and which sites cannot or which are the sites a user from the institute can access, outside. All this traffic flows through the firewall and once you set this rule - accessible, not accessible, those sites will be blocked.

The rule is embedded within our firewall, within our system. So we control the flow of information through specific configuration rules like this. Some of you may be familiar with this, you may have actually seen firewall configuration. This is a technical job.

I do not claim expertise here. This is basically awareness as to what they do. Doing this is a more detailed activity. IDS configuration rules. Intrusion detection systems are systems that prevent intrusion and keep in mind, IDS and firewall are two technologies that actually are deployed to control access. A firewall is something that can prevent access to and from, the system.

You cannot access outside, others cannot access inside. Both the rules can be implemented. So it prevents, it is preventive , it is protective. An IDS is only detection. It is a detection system.

It is an alarming system. Some access has happened, it does not prevent. So that is the level at which these systems work generally. So both are different.

One is for detection, other is for prevention. All right. So that is about my class. Do you have any questions on policy? So we have traversed from policy at a top level to a ground level. We touched the tyre in terms of firewall configuration or IDS configuration as sort of examples to understand how policy is formulated and translated into issues and then finally implemented at system level, at procedural level etc. So now we will discuss an article which was published as a series in Harvard Business Review.

So the first in the series is about Internet security and Internet insecurity. Good. It is not about security but it is about insecurity. So let us listen to the third group who is going to present this. Thank you.