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: 13

Good morning and welcome back to this course on Cybersecurity and Privacy. We have already seen certain fundamental concepts related to cyber security. We have not been under the domain of privacy, information privacy yet. But cyber security as a management and governance issue is what we have been discussing and trying to understand both from a conceptual as well as from a practical point of view. So, we have seen how organizations, unless they have a management approach and management planning built in, as part of the organizational process, how the business can be struck down or the business can be shaken and sometimes go bankrupt, if cyber security is not given due importance. And therefore, this topic becomes extremely important to go forward.

So in the last session, we discussed planning, planning that is required for managing things. So we know that that is fundamental, to manage anything, you need planning, you can do things without planning and you know how inefficient it is. So particularly in cyber security, when the environment is extremely fluid and changing and increasingly threatening, especially if you have a large number of cyber assets in your organization, then it becomes a critical topic. So cyber security requires planning and any planning requires some sort of reference to start with.

How do you prioritize cyber security? How important it is? If I do all the planning, is the organization committed to it? Would they be willing to provide resources for cyber security? We have seen one small incident yesterday, the case of a company called IVK, which did not approve investment in cyber security technology, because it appeared that it is not a priority for the organization. So it is important for managers to know, how important cyber security is as a priority area and do the people in the top management recognize cyber security and its importance ? What is the position? Is it really informed position or is it some sort of arbitrary positions that the organizational top management has taken? So all these are important questions, when we come to cyber security management. So therefore, that brings us to the topic of policy. Policy is actually a document in the case of cyber security, which acts as a reference. Now, let me actually put this question to the audience.

When you hear this term policy, what comes to your mind? What is your thought, when you think of policy, in a very general sense? Use three terms - Rules, Regulation and

Norms. So these three are different, particularly rule is a generic term, but regulation and norms are different. There is something called social norm. For example, come well dressed, come dressed at least. So that is a norm, you can actually decide to dress the way you want or dress or not, it is all up to the individual.

But why do you come, why do you try to come well dressed in the class? There is no rule written anywhere, there is no regulation as such. Nobody can take you to court if you well, dress in whichever way. There is no such thing as regulation, but it is a norm, it is a social norm. What is an acceptable norm? So that is one aspect by which the society functions, you know, largely the society functions based on norms, social norms, you do things because there are others. And that is, there are expectations from the society.

The other thing is the law, law is, regulation is something that is legally enforceable. Somebody violates that particular rule, which is part of a regulation, somebody can take you to court. So that is the point. So, is a policy a regulation? If it is legally enforceable, then it is a regulation, otherwise not. When I shared the course outline with you, did you notice a term called policies? If you read it thoroughly, there is a section called policies.

So policy is something which shows you, what will be the position of the instructor on certain important topics related to the course. For example, plagiarism or examination, examinations. So malpractices, there are strict positions the institute has taken and it is a reflection of what is the institute's position on the conduct of, the code of conduct of students. That is a policy, meaning a policy applies to everyone. A policy is to ensure something collectively, not for specific individual, It is in the collective interest.

For example, if somebody copies, it is and it is okay, if I say okay, you can copy or you cannot copy. I am not fair, I am not being fair, it is about the fairness. So and therefore, you form policies in such a way that certain objectives of the course is met and it gives some sort of balance or equity in the process of delivering the course. So a policy is such a document which an organization develops to ensure that the organization is able to attain its objectives. While ensuring that people are not affected or their personal space is preserved and it does not sort of affect others or it is not imbalanced or unjust etc.

You have to actually take into consideration many aspects, we will go about that. So policy, we all agree that it is a binding document for everyone to follow and it has certain objectives. Now what is the objective of a policy? Policy can either enable, policy can also disable. If a policy is not formed well, it can also disable an organization. As you have already seen in the case of cyber security, there is an organization which does not have a policy at all.

There is no document to refer to as to why should it be a priority, who has said it. Well, there is no document, there is no such thing as something that the organization has accepted and communicated well, down to the members of the organization or in the hierarchy. So let us move on. Well, these are just introductory motivational slides like policy influences progress. So you know there is something called IT industry in India, which did not grow for several decades after independence.

And when did the growth actually start? It started with certain basic policies. There was, you know, policy on computer software export, which actually discouraged foreign investments in IT in the country. And therefore, you know, we thought we can actually develop our own technology indigenously, etc. So there were many models that governments tried out, not blaming them because that was a different time period in history. So then you can see certain landmark regulations like software technology parks, and economic liberalization, etc.

, are broad country level policies, which encouraged an industry. In the absence of that policy, the industry may not have grown. See post, you can see, when did actually India's IT industry start growing? You can see that major change happening from during this period. That is, when there was new economic policy and foreign investments in IT, IT industry, IT exports, IT services exports, all became possible because the policy allowed it. So and then we are very proud of an industry today.

It has come into being, because of a change in policy. So policy influences progress, that is at a bigger scale or a higher level, at a country level. Policy can also influence behavior of organizations. Policy can also influence behavior of individuals. There are several studies on employees' compliance with organizational policies or cybersecurity policies.

Organization may formulate some cyber security policy. But sometimes the policy can be so, policy can make your day to day functioning very difficult. For example, you are not given an internet access in the organization. And then, if you do not access the internet, maybe it is for the purpose of security, but you find it very inefficient doing certain activities, getting certain search done, or you know, referring to certain important websites, you cannot do that. And sometimes the timelines, deadlines given by the boss may be very tight, but you do not have access to resources.

And it is seen that people violate policies. So policy violation and policy compliance is a function of many things. And therefore, if the policy is not well framed, taking into consideration the objectives of the organization. If it hampers the objectives and make it very restrictive, then also, it is not good for the organization. So, one thing is to protect,

other thing is to progress.

And this is the trade off that we discussed already that when you make your intuition detection very active, then it affects your efficiency or if the logging is turned on, it is good from a safety point of view, but inefficient from a functional point of view. So I will show you the term of reference given by government of India to Justice Sri Krishna Commission, who first framed our data protection, but your personal data protection bill. So the government said, protect the privacy of people without inhibiting the potential of digital technologies. So digital technology should be used, but at the same time, privacy should not be compromised. You know, these are like two parallel lines.

So the purpose of regulation is to bring a balance between these two. Whenever there are two parallel things or conflicting things, you need regulation to bring a balance. So that is the, so policy is embedded, of course within regulation because regulation is legally enforceable. Policy need not be depending on the context, but regulation is basically a policy. It actually directs how a particular domain or a particular issue should be addressed or conducted.

So therefore, if a policy is well framed, it can motivate people and invite the right behavior. If it is ill framed, it can actually make people rather violate the policy. So if it induces fear, for example, a policy can induce fear, if you violate, this will be the consequences, there will be huge penalties, punishments, etc. people may comply and keep in mind when people comply, they are complying for the sake of the regulation, it will be at the cost of work output or efficiency etc. So therefore, it is a very important topic, how you bring the balance between efficiency and safety, in the context of cyber security policy.

Now, with that introduction of policy as a document that is developed and implemented for ensuring the objectives of the organization, ensuring safety and security of assets, it is an essential foundation for effective cyber security programs. Without a policy, when you have doubts or crisis, there is nothing to refer to. Suppose there is no constitution for India, then what happens, you can imagine, there is nothing, why, how can an institution like IIT Madras function unless there is a constitutional provision for it, everyone can set up their own shops and make all sorts of claim because there is no reference. So, you need these fundamental documents to ensure what we want to achieve and to prevent what is not expected. So, you see the next point in the slide indicates certain important principles in cyber security policy formation.

In all policies these apply, but we can look at it from the specific context of cyber security policy. The number one, is a policy should never conflict with the law. A policy is

formulated in our setting for an organization, a cyber security policy is formulated for an organization. And certain sectors by regulation, it requires that there should be a cyber security policy, Banking institutions is an example, RBI requires every bank should have a cyber security policy, defining structures, defining processes. Now when you formulate it, it should be in line with, compliance with, regulations and the law of the land.

An important case in point which is referred to in your textbook is that of Enron Corporation and Arthur Anderson. Have you read about that scandal - Enron scandal in 90s? I was working in industry that time, it was an event that shook the whole world because major accounting fraud by Enron. The company was going bankrupt and they had an auditor and that was Arthur Anderson. So audit means, you know you audit and say the company is very healthy. So audit is going on and audit reports are produced and the company's work is going on, but actually the company is going through major fraud and scandal and it was not detected or reported.

And that is when the government woke up, not only in the US but all over the world. Because a company can go bankrupt if there are no regulations or standards which are publicly available for people to scrutinize. So mandatory reportings, compliance with certain accounting standards, Sarbanes Oxley Act, all got the regulation, got stricter post that event. But during the incident, something happened.

So of course, this went to court. So Enron and Arthur Anderson actually had to give their response to what happened. So Arthur Anderson wanted to wash their hands and say we are not responsible. Something happened whenever we, when we audited everything was fine. But what happened after that, you can always say, you know, we found everything fine.

It must have happened afterwards. So what Arthur Anderson did was, it destroyed all documents of evidence which was related to the audit. For example, emails and documents. So then they framed a policy known as shredding policy. Shredding policy is, at what frequency you destroy your documents. Our, I think our institute has a shredding policy.

The examination answer scripts need to be retained for four years, I believe. And after that it can be destroyed. So they periodically come to collect the answer scripts from us and that is the shredding policy or retention policy. So Arthur Anderson framed an interesting policy known as any document need to be retained, to the time till it is relevant. So that is a very, not an year, not a number, till it is, who decide, whether it is relevant or not.

Once you make a qualitative statement, then it is subject to interpretation, who interprets it. So one can say, well, it is no more relevant, the audit is over, everything is fine. So we just, so actually they destroyed all evidence pertaining to the audit by framing a policy that a document can be shredded or destroyed after it is found not relevant. Now the point was, it was seen as a destruction of evidence because it was seen as a policy that is in conflict with the law. And today you see, there are strict regulatory requirements to retain evidence say in telecom and in several sectors, not qualitatively but specifically in terms of numbers, which are measurable and which are without dispute.

So when you form policies, it should be in compliance with the law. This is one example. I am citing another example which is at the bottom of the slide. That is, I think all over the world, child pornography is illegal by law, in any country. Now suppose, you have access to internet in your organization and someone say is addicted, you know this is personality disorder, somebody is addicted to some form of pornography and these sites are accessed from the organization.

Who is responsible? Is the employee responsible or the organization responsible? Organization, employee is not responsible. Both are responsible. Individual is responsible understandably. But why should the organization be responsible? It is the individual who, say internet connectivity is provided for accessing sites that are required for work. If somebody did something wrong, then that individual should be responsible, why organization should be responsible.

Yeah, but organization can say in the code that we have to let employees access internet for work. And if we stop that, work cannot be done. And if an employee accessed a site which is illegal, that is the employee is responsible. We have to give internet access because that is required for work. Any different opinion? Is organization liable or not liable? That is, why should they block because anyway it is understood it is against law and you are you know, even otherwise individually we are not supposed to access such sites.

You know the National Law actually, IT Act actually prevents to the best of my knowledge. So why should the organization care about it? It is at your individual risk you are doing it. Yeah, that is true but the organization should take an effort from its side to block the sites. Yeah, so the point is, the organization can make a claim in the code that it is individual's fault, if there is a policy. Based on what are you saying? Well, it is understood, it is there in the law.

No, do you have a policy which clearly suggests that the access to internet is for work and employees are not allowed to access any site which is prevented by law ? That is a

policy. There should be clear policy statement, then say well, here is our policy and this individual has violated the policy. Then it becomes a stronger argument plus policy implementation. One is to frame policy, other is policy should also be implemented. And the organization also has to take due care in implementing the policy.

That is where your argument becomes valid. Well, block the sites which are not supposed to be accessed by law, Then your argument becomes more strong by saying that well, we have done due diligence in our firewalls, these sites cannot be accessed. But the problem is, there can still be sites which come up every day you may not be updated that some sites can still be bad sites which people access but then you have policy. It becomes policy violation. So therefore, a policy, a cyber security policy should be in line with the law of the land and it should have provision to, if you give internet resources or cyber resources to employees, the policy should ensure that it is used in accordance with the law of the land.

That is organization's responsibility. That is one thing to keep in mind. Are we following the law? Have we, do we have all the clauses to ensure that laws are not contradicted or confounded as in the case of Enron, where they had a very convenient policy, which is not acceptable. So, it should be able to stand up in court, that is the consideration. So, you may work tomorrow on policy, on you know it may not be cyber security, any policy. A key principle is do not contradict the law and it should stand up in the court tomorrow.

So, you should be aware of providing laws and regulations related to the topic. And it should be properly supported and administered as we said, you know the firewall should actually not allow access to those sites. And policy should encourage, this is the negative side and policy should actually encourage success of the organization or in attaining the objectives of the organization. So one thing can be to block access to internet, then how do you work? So you have to give access or you have to tap the potential of digital technologies as the government said, at the same time without compromising privacy, You know, that is a big call. So that is why we see you know that it is a never ending debate to form policies on privacy.

And involve end users of information systems in policy formulation. Well, this gives a picture of where policies and you can see that in this, a policy is in the outer side circle, meaning that policy is referred in all the cyber asset related activities of the organization right from networks, individual systems and then specific applications. So, policy is a binding document.