**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: 01**
**Lecture: 03**

Okay, let me actually ask this question openly. What do you mean by security? Leave cyber security. So the course deals with security. Protection from threats, protect whatever is important to you. Okay, Is there anything general? When do you feel secure? The general meaning of the word secure. Okay, okay, let us talk about general physical security.

Let us also include not just information security, but physical security. Feeling safe, feeling safe. What is that feeling? So the point is security is a psychological sense as well in the general sense. Information security has also a emotional dimension but as you pointed out, it is a quality or state.

In a general sense, security is a state, a state of being safe or state of feeling secure. Well, everything is fine. There are no miscreants, there are no people who are trying to, you know, attack or intrude and cause damage to your property, your assets, your information or yourself, you are safe. So these are the constant concerns we have for our survival. So when we change the unit from individual, so I asked you a personal question, in fact but when you go or change the unit from individual to organizations, organizations also have assets to protect.

For us as individuals, we are the asset, my body or my life is the most important asset and then my information or what I carry in my mind, you know, that is the next asset that I have as a individual, but it is a whole. And for organizations, they have plenty of assets, physical assets and informational assets and that used to be the scope of cyber security or information security in the past. And that is why I said when cyber security is referred to, the general understanding was it is about securing information. It is about securing computers. It is about securing computer networks.

And that is the scope, nothing beyond that. But today, the scope is also about securing what is added to. So yeah, we are coming to the definition of cyber security versus information security. In information security, as I said, you protect information as an asset, data and information. For example, your databases, like in AIMS servers, you know,

people got access to AIMS database servers, that should not happen.

It is a breach of data. So and therefore, it is related to information security. So can you imagine what would be the added dimension in cyber security? Information security is a part of cyber security. But when you refer to cyber, there is a little more or in fact, there is much more. There are different aspects of security when it comes to the organizations.

When you discuss organizational security, there is physical security of various infrastructure elements of an organization, then there is personal security, operations, communications, network, information and so on. So that is security in general. For example, before you enter the institute, IIT Madras, there is a gate. There is a gate and what is the purpose of the gate? And there are security personnel deployed there. So, the institute has invested in creating a gate, we call it a security gate.

And we have security people deployed there , 24 by 7, essentially to ensure security of all that is mentioned here. It is about the assets of the organization. But how are they ensuring the security or what is the role of that security? So, that is where the discussion of how security is ensured or what does a cyber security do? So, one word is definitely, you use the word verifying, you said authorized access, etc. So, we will discuss that more systematically, what does cyber security do? But essentially, a security system ensures that people who enter the campus are authorized to enter the campus. Those who have the right to enter, only enter and others do not enter.

Or conversely, those who have the right to enter should be able to enter. They should not be denied entry. And those who do not have the right to enter, should be denied entry. So, you can also see false positives and false negatives can happen there,in security system. But their role is to ensure that.

But if that has to be done, then they need to know who is who, Who is trying to access, whether they have the authority or not. So that is a verification. We will get into the details of how cyber security is ensured. But there are some confusing terms here like cyber security versus information security That is one. Otherwise , of course, let us look at, you know, the words,you know, we should be very clear about the basic terms that are used, the dictionary meanings in fact.

So, there are two words cyber and security. What do you think- which is correct? There are three ways in which you can write cyber security, cyber security with a space in between, cyber security with a hyphen in between, or cyber and security together, which is correct? Hm? All are correct. Okay, good. Okay. So you probably you say all are correct, because you may be reading so, in in different articles of papers.

Is that so? Okay, let me see how I wrote this in the title. I gave a space in between, cyber and security are two words. Is that okay? Okay. A is more common in reading.

A is more common. Okay. Well, you are right. All the three are correct. But only one, only one condition. If you use one convention, like you write cyber and security separately, follow that consistently.

In the same paper, you should not use different forms. If you choose cyber security as two words, which is the norm in in Europe, typically in Europe, they use the two words differently. And then follow the European convention. The last one is the US convention, cyber security is written as one word. And if you follow that, then you follow that consistently, it can be written as one word.

So therefore, if when you read journals or articles, which originate from the US, you will always see it is a one word. But if it is European, you will see these are two words. So you can follow any, so there and in India, we reach a compromise, the compromise is B, you put a hyphen, because you do not want to displease anyone. So, that is also fine, in some literature people do so. But adding a hyphen, instead of that you can add a space or whatever you you think you like you can, there is no problem, but follow one consistently.

Now the word cyber security - cyber. So and the word cyber, we need to understand that correctly. Cyber is a word that became associated with computers or the networked computers, or predominantly the internet and the world of internet, I would say from 90s onwards, the cyber world, we use that word cyber. It is a prefix to many words. Today we have cyberspace, cyber coolie, cyber world, cyber cyber.

So this cyber, well, I do not know who did this, because the word comes from cybernetics. Cybernetics is a Greek word. And cybernetics actually means somebody who is steering a ship or a vehicle, the steerman, someone who is in control of that. So cybernetics means control. So that is one word, you know, in Greek it is one word.

So somebody pulled cyber out and used it to represent the internet. So internet connected world or internet connected systems is generally referred to as cyber systems or the cyber world. Just keep that in mind. It is a new, it is a new terminology. And cyber security in that sense, since it connects to the computer systems or networked world, it denotes the security of the networked world, the computer networked world.

So, that is the connotation in terms of word meaning - cyber security, cyber denoting the internet world. And cyber in terms of netics, it is cyber security means security of the

world of internet. And that is where actually we differentiate cyber security from information security and for your information, International Telecommunication Union, which is a global body for telecommunications, digital technologies, old body. They have in 2008 given a definition to cyber security, which I have reproduced here.

It is not from a textbook. But it is a kilometer long. So, they are trying to include every aspect of the sphere of computing, every element and every aspect of sphere of computing, which includes tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, technologies, all that is related. So therefore, you know, many of them are correlated. So the definitional clarity is, is an issue, but cyber security is all inclusive, the security of everything that is under the cyber world. And therefore, cyber security would also involve users or human beings.

Do you think that is a concern? It is not just the information, but you as a user or you as a user, having an account in a social network like the Facebook. One thing is, your profile should be safe and no unauthorized access should happen. Well, that is an information security concern. But there are other concerns about security, which is your own security in the cyber world. You know, there are cyber attacks on individuals.

There are movies today, right? People have been bullied or the so called cyber crimes. Our TA is Binod, so Binod's research is related to cyber crimes. So there are criminals in the cyber world, who can actually cause physical damage to you through these channels. The security of individuals from cyber crimes is a concern or it is a part of cyber security. It may not be information security it is a bigger scope.

So, in definition, I would say, cyber security is information security plus individuals. For example, if there is a drone attack, well, the drone has surveyed your premises and there is of course, leak of information, they have done intelligence, but it is going to attack me, it can kill me. So, my safety through technology, through the use of technology or information technology is also under the purview or under the scope of cyber security. So cyber security covers everything, users and systems. Information security is more about the systems and their security.

Now, since it is an emerging phenomenon, we will borrow a lot of concepts from information security because the concepts have been developed well in the literature of information security. And I am going to introduce the course outline to you now. And you will see that your textbook is titled information security, okay, information security So,it is predominantly the textbook deals with information security and other aspects of cyber security will be covered through extra reading materials, which I am going to give you. So, we will be covering both the aspects of information security and security in the

cyber world. And as I outlined, the cyber security seeks to ensure three aspects or security can be understood in three elements, confidentiality, integrity and availability or it is generally known as CIA, CIA triangle.

There are three dimensions of security - information security. And I will be dwelling on these three concepts in the next class. We will try to parse out and get into the details of what is confidentiality, what is integrity and what is availability. And these pertain to information, confidentiality of information, confidentiality, sorry, integrity of information and availability of information. That is the purpose of information security management.

Yeah, so the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information. This is a definition of information security. Information security definition as given by Whitman and Mattord. And this you have the 2018 book, which is your textbook by Whitman and Mattord , one of the leading textbooks in the field of information security management. I must caution you about the expectations from the course, as I take you through the course outline.

Information security can be taught as a technology course, from the computer science perspective. Information security can also be understood from a managerial perspective, management and governance perspective, where technology is one aspect. Technology does exist. And we need to understand the role of technology in cyber security management.

But it is not a study of technology. Cyber security is much more than cyber security technologies. So, this course as outlined in this textbook 2018 covers the management and governance aspects of cyber security management or what managers should know about security of information assets and security of other assets like including people in an organization will be the predominant focus of this course. So for example, cryptography. A CS course may dwell on cryptography for several sessions because that is an underlying technology to ensure confidentiality. When information is transmitted from point A to point B, node A to node B, the node A sends that information to node B, to be read by someone.

And the purpose of cyber security is to ensure that only person who to whom it is addressed, to whom it is intended, should read that information and nobody else. And that is confidentiality. And the role of cryptography is basically to ensure that nobody else reads it, even if somebody accesses it. You cannot sometimes prevent access. You know, I am talking to you and all of you understand.

I hope most of you. Is my English okay? I guess in India, my English is okay. Well, we

have some different pronunciations in different states but by and large I am, okay. Why do you understand me? Same medium of communication or same language. We see language X is based on a shared understanding of the words and the structure of words is the grammar. So, you and I understand most of the words I use in a similar sense.

And you also know, when the words are connected what they mean. So, we have a shared understanding. and therefore the communication happens. But if I use a language, say I use Greek, which nobody understands in this class, I may be teaching the same thing.

You are here, you have access. You are very much listening to me. But do you get what I am saying? You do not understand the thing. Maybe from the body language you get something but in the world of computer transmission there is no face expression. It is only the text or it is only the information. You do not get anything out of it because it is another language.

You call it deep encryption. Because it is encrypted even if you gain access, you cannot understand. So, it is a very important technology from the technological perspective. But when we look at, I am just giving an example. When we look at encryption, we try to understand what are the different types of encryption and how they are used? But we will take the application perspective. What does encryption do, than how encryption algorithms work? That is the technology domain.

So, we look more from the applications of technologies in cyber security management. And I will have a case study in the next class, which would actually help you understand clearly. Is cyber security a technology problem or is cyber security an administrative problem? But if I raise that question now, what would be your quick thoughts? It is both. It is more an administrative problem. What makes you think so? Because it is a technology that is attacked most of the times and it is the technology that is used to attack.

So, therefore the focus should be on technology. Technology as a tool and administration as the framework or administration as something overarching which deploys techies. So, that is actually a view which techies may not appreciate because they say , they say today, we are moving towards zero trust systems. Zero trust means no trust in human beings, trust none. I have some articles on that. So, you have to develop and deploy technology such that you do not have to be dependent on anyone's credibility.

So which is actually an approach where humans are less important or the technology takes you know, gets a higher importance in managing cyber security. That is a good debate and we will see as we go. So these are actually opinions that you have in your mind about what cyber security is whether the management is more important or

technology is more important. But some of you argue, both are important. So let us examine certain important cases of data breach that happened in the recent past and that will be an important ingredient of this course.

We analyze cases to understand what went wrong and what action was taken subsequently. And then you will understand cyber security as a more complex problem and data breach of big organizations has not only technology issues but huge administrative issues. And you will also see that has regulatory implications. Government wakes up, when they actually see instances of data breach. So, it is not just technology problem, well, it exists at some stage.

It is an administrative problem at the organizational level. And it is also a regulatory issue, in when data protection is not regulated. There is no one to question you. So, why should some company invest so much in cyber security or in data protection. So, the law of the land also becomes important. And you must be aware our country is today debating a personal data protection, as a law, as a bill.

Of course, there is politics in it but you can see the criticality of the issue today within the digital world. And have you heard of GDPR? Very good. So, you can see that it has gone beyond administration to policy and regulation at national levels. So therefore seeing cyber security as a narrow firewalls in putting up intrusion detection systems or firewalls or whatever protection mechanisms at the technology level, well, it is a important element. But there also need to be administrative and government systems and standards.

Standards to manage cyber security and also policies and regulation to govern at a country level these issues. So that is what cyber security and privacy today are. So, in this course let me actually take you through the contents of the course. Maybe what I will do today our time is almost up. In the next five minutes, I will just give you a very brief overview about the course.

And maybe the course expectations as to what you are supposed to do in the course. I will explain to you maybe a little more, in the next class. So, the philosophy of the course is what is outlined here. And I have posted the course outline and the course extra reading materials in Moodle already.

So, you can gain access to it. So, there are mandatory reading materials which are related to the course. And there are also supplementary readings, which are research papers or articles and even videos that actually would help you develop understanding about cyber security, which is posted or referred to in the course outline. So, let me end with the course learning objectives. Course learning objectives are fourfold.

There are four objectives from this course. Number one , to recognize cyber security from technological and administrative perspectives. So you must see that it is both. It is not just one. And in this course, I am not going to sort of ignore technology.

And just make it a management talk. But we would definitely look at technology as threat and technology as asset and technology for protection. So all the three aspects of technology would be covered in the course. As I said, it has a threefold role in cyber security. And I must also say that I am not the expert in cyber security technology especially from the protection mechanism point of view.

So, that requires a lot of technical knowledge and experience. People are do exist in the domain who are experienced in cyber security technologies. So, as part of this course, I will be bringing in someone who can talk about cyber technologies from experience and involvement much more. And that is a part of the course, a part of the pedagogy. So, you will have a guest talk from industry and all your doubts, you should actually ask him not me. In the sense, this is more like a sort of interaction with a cyber security practitioner.

That is the understanding. And so, how is this CL01 the course learning objective covered in the course. I will just take you to the session plan. You can see, I am covering foundations of cyber security, information security and related concepts with the help of your textbook and also research articles, principles of information security management, confidentiality, integrity, availability, etc. What do these concepts really mean? That will be covered in the next session. So, this is about cyber security fundamental concepts and you will have a case study of Target corporation.

One of the defining instances of cyber security breach was in 2016 alongside the same time I think it was 2014 when Sony Corporation faced another huge data breach. These two together actually shook up the world not just these companies, not just industry but government as well. Because cyber security has become much bigger or in terms of size and impact. So, that is why I have selected a representative case of the Target corporation and we will analyze that case.

Security management, governance, risk and compliance. So GRC generally there are frameworks. There is an ISO standard, there is GRC framework, which can be implemented by organizations for overall management of cyber security. So, instead of looking at it bits and pieces, buying some updates on a new technology, how do you actually implement cyber security as a practice, as a management framework in an organization and becomes compliant with certain standards. So what are those standards? That will be one discussion in the course. And then, let me actually put it in your mind

right away from a cyber security management perspective.

Management is about planning, management is about managing resources at a fundamental level. So there are two types of planning. One is called contingency planning. Contingency planning is to manage contingencies where the basic premise is despite all the steps that you have taken to protect your systems, things can go wrong.

Contingencies can come. Planning is done by human brains, who cannot predict the future completely. You can have some prediction but predictions can go wrong. Then what do you do? That is contingency. So, contingency planning is one dimension of cyber security management.

The other dimension is the risk management. In risk management, there is no assumption that something has gone wrong. But the assumption is something can, what are the things that can go wrong? And how do you actually protect your systems against that? So, one is about proactive or you know sort of preventive. Risk management planning is about preventive. You prevent your systems from all potential disasters that can happen.

Contingency is about reactive. Suppose something go wrong, how do you do the firefighting? How do you fight the fire, that is broken up? And then things restore the systems to normal operation. So fundamentally I would say cyber security management deals with these two aspects, contingencies and risk management. So, these are the two important aspects we will be covering from a management perspective in this course. And then there is cyber security policy which is a reference top, reference document for understanding priority for cyber security and resources for cyber security, etc. So, as I said, we will, I will take you through the foundations, fundamental concepts and also, we also look at the technologies for cyber security.

So as I said, there will be a guest lecture, security technology, cryptography and security I have dedicated one session to outline. So, I will be doing that from a confidentiality point of view. And there is also something known as passive defense versus active defense today. A lot of technologies are actually deployed for passive defense,to protect.

So, you also have heard offense is the best defense. Can you offend the hackers? Can you attack them, instead of they attacking you? That is just a thought, but active defense, you go beyond being, you know, building walls, you go beyond that, you tried shooting. So that is the, so but what are the legal sides? I know you must be very aware. It is not a, it is not a trivial thing. And then you can see the course slowly moves from topics related to cyber security to privacy, Information privacy, and its landscape and one of the important things this course does is to familiarize you with the landscape of regulation,

privacy regulation in different parts of the globe.

So that is, and including India, North America, Europe and India. And so, there are several cases that I will use to illustrate this and help you understand the concepts clearly. So that is what the course is. So I will thank you very much. Have a good day. Thank you, sir.