**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: 01**

Good morning and welcome to this course - Cybersecurity and Privacy. I want to welcome you and I thank you for signing in for the course Cybersecurity and Privacy. Today is the day of introduction and therefore we will be breaking the ice and also get to know what the course would contain, in terms of contents of what I would deliver from this course and what I expect you to do as part of this course or the coursework. These are the two main things that we will discuss but I will also try to motivate you about the topic. So that is very important when we start- Is this topic important? Is cybersecurity an important topic? And should it really bother or should it really be a matter of concern for practising managers, irrespective of what you manage? Should managers be concerned about cybersecurity? And if so, why? That is something that we would try to address in the first session so that you have a clarity of why one should credit a course or why one should actually spend so much time going through a six credit course to do, to understand cybersecurity and privacy. So the title is Cybersecurity and Privacy.

I just want to know what is your understanding about cybersecurity? So you can just talk about, what do you mean when you hear this term cybersecurity? There are two terms- cybersecurity and privacy. So it is an "and" there. So feel free to talk about it. As to what is your understanding? So, cybersecurity is more about vulnerability management of the computers and the network system, so that the data whatever is there that gets protected and you know unauthorized use of the data without the knowledge of the owner.

Okay good. So you have three keywords. One is data, other is about vulnerability, third is about unauthorized access. So these are certain key terms that is associated with cybersecurity .Anything else? Any other thoughts on cybersecurity? Okay, what do you think about privacy? That is the second term.

See, the title is actually consisting of two key terms- cybersecurity and privacy. Okay good. So we talked about two things one is privacy,is about me and my data which I choose to disclose, I choose not to disclose and other is the security layer which exists at some level, some system level. Alright, so there are two things cyber security and privacy and the interface or the intersection between the two is also important. So, how is cybersecurity and privacy related? So that is another aspect of the course.

Okay, let me actually give you some more background information as we go, to get a motivation to understand- Is cybersecurity and privacy a current topic? Is it an important topic? And is it relevant to managers? So, here is an email I received some time back from the director of IIT Madras and when you receive an email in your official emailbox and it is from the top boss,you pay attention to it. So his name is written and it is a request and there is content of course to meet him and of course it ends well, best regards, name and designation, right. So what should I do to this email? And I know Professor Ramamurthy ,he does contact people when he wants to give some specific roles or administrative roles particularly ,he did have this habit of calling up people or writing personal emails and doing like this. So this is an instance of that kind. So what should be my response? I should check the email id.

Why should I do that? Because you know ,we do not check the sender id when you get an email from your colleague or from your area head or department head .We just have a lot of communications going on. No. How, why should I doubt this mail? Sir, there is no need to be suspicious according to me because it does not demand anything like sensitive information from you, just asking you to drop an email. But I must tell you, I did check who sent this mail.

I got suspicious. Can you imagine, what is the source of suspicion? This is? Well, that is okay. It is an internal mail, so this is fine. The signature part is fine, the address, everything is fine. Okay, it looks informal.

The pattern is different from the other way of getting the same. Okay, yeah, I agree with you there is a slight change in the pattern, this is written like a very personal mail, you know, there can be some personal element when people write you professionally. But more than so but it is very personal. Can I have a quick, that is also fine,moment please. So this does not sound professional ,as you sensed, I also sense you know I do not expect him to say-" Can I have a quick moment with you?", right.

So I became suspicious at that particular content. This cannot be from the director, okay or this may not be from the director because this is not the choice of words when you typically write to a colleague or in a professional setting. So and then, of course, as you suggested I decide who is sending this email, of course that is the first check all of us can do when we have a doubt,okay. And I found this email coming from a Gmail, not from the IITM domain and therefore this is obviously suspicious and we call this kind of mails as phishing mails. We typically call it phishing mails, but it is not just a phishing mail.

Phishing mail, all of us get every day, in fact a lot of junk mail comes asking for our bank details or other kinds of personal information. We know that this is obviously phishing

mail but here it takes time to resolve this because it is a colleague or it is a director and his address is given at the end. And the sender also knows that, well, I am a faculty member of IIT Madras and Professor Bhaskar Ramamurthy is the director, of course, the former director. So someone knows, who is who, in an organization okay. Somebody has actually collected background information, okay.

We call it typically social engineering okay. So, this is social engineering based phishing mails, where the chance of one responding to this is much higher, okay. So not just a phishing mail someone from Africa writing ,I have a lot of funds to transfer why do not you share your bank account details. We obviously know, I do not have, I do not know anyone out there but this is from a non-circle based on social engineering and this is called spear phishing ,okay. Spear phishing is very specific ,based on social engineering where people or the hacker or the hands behind this, have done background study, okay.

So then subsequently of course, Professor Ramamurthy sent a follow-up mail to all the colleagues because he knew that this phishing mail was circulating in the institute ,okay. So, this is sometime back and this is very recent, okay. So ,couple of weeks back, the head of our department wrote, again a similar mail- "Can you do something for me?" right. And here,again you see, the professor, you know, the proper title of the faculty member, the name and the signature, you say it is full signature. So, you usually tend to reply immediately, okay.

So, what I essentially want to say here is that, we face this kind of problems or this kind of threats in the world of internet, in the world of so called, cyber world often and it is all part of our experience or it has become part of our day to day experience. What I am trying to do is to sample, to sample some instances which I came across either individually or from newspapers and to give you a sense of what is going on in the environment in the current times, okay. This is a text message I received,you know, in fact two weeks back and the text message asked me to do a verification of my PAN card, okay and it gives a link to the SBI site and I am sure all of you have,most of us have our account in the State Bank of India,okay. And of course, since this is request from a bank, you tend to respond to it ,right and it led me to this site, you know SBI and this login page looks exactly the same, okay, the bank logo and whatever fields you generally fill in, in the same font, in the same format is given and then you have to enter the captcha code and looks like I should be entering this data and signing in, to do whatever formality is required to keep my account on. But is there a problem here, I think by now all of us or most of us are familiar, so when you get a message to sign in somewhere, you go and the first thing that you look is what is the what is the website, is it giving the right address or it is giving a fake address In this case, we know that this is not SBI website from where we sign in, it is online SBI, but it is something else.

So, as soon as ,even when I sign into a bank account on a regular basis, I of course check the address because sometimes a wrong address may pop in and we may be signing in and the signing in data including your username, password may be going elsewhere. So, yeah, let me continue this so, I just show you some things I faced as an individual, okay as an individual or of course this phishing mail is something that went to everyone so as a group or as an organization, we do come across instances of cyber security or cyber security related issues and these are clips from leading newspapers of India where it recently reported increasing number of cyber attacks, okay. And the last piece is about ransomware attacks, have you heard of ransomware attacks? okay but denial of service attack is different from ransomware, we will be we will be discussing a case on denial of service but ransomware is a, is another kind of a security threat where the one who attacks, so the hacker, takes control of your machine and encrypts, in fact encrypts your machine and ask you for money to release it. It is like when you lock your house and go away and when you come back you find that your house is, there is another layer of a lock on your house and you cannot enter the house because somebody else has locked and the hacker is quite fair, well, I will give you the key to enter but give me some money, okay ,and let us not make let us not make it complicated, just give me some money, the key is with me- take the money, take the key, unlock and go in, okay. So it is ransom, you know the word ransom is, about you know, it is about paying to release someone ,okay ,so ransom redemption etc related words, so you have to pay a ransom to release your machine from someone else's control,okay, ransomware infact ransomware is one of the most frequent attacks, in terms of threat intelligence in today's world,ransomware has become very common and this is something about which the world,as a whole is concerned about, okay.

Here is a report ,again from newspapers, as I said, this is another sample which happened predominantly in the western world, where the POS machines, you know, the POS machines are typically in a retail store, when you buy something and when you check out ,there is a POS point of sale machine, where you actually do the checkout process and make the payment and then take your items and come out, but if suppose in a very busy day on a retail store if the POS machine stops working, okay, then you know the kind of chaos and also you know the operations just stop there because companies which are automated, they would not have a manual process to continue business, okay. So your shops just close down and this did happen in 2021 when retail stores which used the POS software built by Kaseya,okay, Kaseya is an IT company which provided POS solutions and several retail stores in the west stopped because there was a ransomware attack, you see, what is the ransomware attack- the hacker just want 70 million dollars to restore the machine and the most of the times, the hacker is very is a good thief, you know you call it good thieves, you pay the money and it is done, you know, the machine is released but if you do not pay the money it is, it is very very difficult, okay, to become operational and

generally in my reading, I found that companies just pay the money and restart the business okay. The only exception I came across is in Chennai, okay, so Chennai corporation's PC's were attacked by hackers and it was a ransomware attack, okay and Chennai corporation refused to pay the money, okay, because they found that the machines were very outdated ,okay, so they were running on windows 8 and it is very easy to take control of machines which are not updated with the operating systems and they said ,okay, let it be locked forever so they did not pay but for critical business operations when ransomware attack happened ,okay, so it is huge loss, okay, so per hour loss will be very huge as compared to the ransom that the hacker is asking for ,okay. So and that has become a serious nuisance in today's world and here is more report so I am not exactly following a chronological order in actually presenting to you the different cyber attacks that happened in the recent times but this is November-December 2022, you must have read this in newspapers about All India Institute of Medical Sciences. So, five servers were hacked by the cyber criminals and they took control and you know the biggest concern when a hospital's data center gets, comes under attack, okay, this is a different type of data, this is healthcare data,okay, and someone takes control or someone gets access, you know, you said unauthorized access, okay, somebody gets unauthorized access to my personal health data, okay, in India we may not be so concerned about health data but health data when it goes into the wrong hands has huge implications ,can you imagine why,so much so that in the US, there is a act called HIPAA, okay ,so that relates to healthcare it is a regulation for healthcare data alone, why is the world so concerned about healthcare data protection, can you can you just imagine and give me some quick answers, once you have a health condition.

So health care data is super sensitive because the the person whose health data is leaked the the person actually faces huge embarrassment ,okay and it the person also can face losses in an organization or it may have higher consequence and that is why the top hospital of the country when their servers were attacked or came under cyber threat, it became a huge concern, huge national concern. So we see cyber attack happening in all spheres, you know, all domains, it is not just, we just saw Kirloskar, you know ,it is a manufacturing company, we saw AIIMS healthcare, these are all very recent news, so you just open the newspaper, everyday newspaper this is what I see , there is some piece of information or some, something that is covered about cyber security, almost everyday, okay. So we all talk about digital world,digitization, digital India and so on, so you see a very bright side of how digital technologies are actually enabling the growth of the economy or enabling the country to actually progress, be in the line of progress, we also see alongside a dark side,there is a bright side- very bright side of digital and there is also a dark side or the dark world that develops alongside and that is the concern of cyber security okay, so the world consist of good people and bad people, okay. So there are bad people in the world ,who understands the weaknesses or as you use the word vulnerabilities and can exploit

those vulnerabilities very, very well and damage, cause damage and losses the impact of such actions can be very high ,okay, to the extent that the recent, I think this is E&Y report, which is summarized in the newspaper, which shows 91 percent of the organizations reported at least one instance of cyber incidence in an year, at least one incident. So think about that 91 percent of organizations do actually face at least one incident an year, okay and it goes on to report how cyber security is becoming a top priority for CEOs or leaders of the organizations.

So this is, the this piece is of grave concern to me, okay, so you know the changes that is happening in transportation.