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: 02
Lecture: 05

So, there should be straight recall of these three concepts. Let me illustrate it with an example. So, there is an image of course, what does it take you to, this image? Biometric the, yeah, the retinal. So somebody is taking a biometric scan of the eye. It can be different aspects of the eye, we will see that later. But you all have an Aadhaar card.

So you all went for Aadhaar identification, that was the stage of identification. So, the first concept related to cyber security is confidentiality. And in order to ensure confidentiality, one of the first steps is identification. I gave the example of the security gate.

Security gate, if people come to the security gate to enter our institute, the security actually decides whether someone can enter or not. But how do we, how will they decide whether you can enter or not? You cannot simply look at the face of people and decide. You cannot just look at if somebody is smiling or somebody is well dressed or not well dressed, you know, these are not ways. There has to be some credible mechanism by which people can be identified. Without identity, you cannot ensure confidentiality.

Who is who? Whether somebody is given the right to access or not, is based on identification. So you can see that in all data collection efforts, be it by government or by organizations, the first step is to create identity. As soon as you join IIT Madras in your initial enrollment process, there is an identity creation process. You provide your data and you provide supporting documents and based on that, the administration actually agrees or they have those processes to identify you. And based on the supporting documents you have given, you are given finally an identity card.

So how will you enter IIT Madras if somebody stops you at the gate? Here is my identity. And that identity card identifies each of you as a student,as a student of IIT Madras. But if somebody stops me, I also have an identity card and I show that identity card and I am identified in a different role. I am not identified as a student, I am identified as a faculty. You have your ID card in front of you.

So a student of IIT Madras. Well, a student can enter. Of course, the dates are also important, not an old card. So they check that and that they let you in. But if there is no identity card, they cannot actually make a decision, it becomes very difficult.

So the first step in confidentiality is identification. Identification is the process of creating credible identity for individuals who can access computing resources. You can imagine the effort done by the government in creating an Aadhaar ID for you. The most difficult stage is the identification process. Because government had to use vendors, existing vendors and the government verified their credibilities and outsourced this job to vendors to create identities or to collect identity information and finally assign an identification number, which is called Aadhaar number to every individual.

That was the identification process. Identification process, creating an employee ID or a role number or an Aadhaar number, an account number, all these are actually part of identification process. So the first step in security is identification. Who is who? And the second step in confidentiality or in cyber security in general, it pertains predominantly, to confidentiality. So that is why I am saying it is linked to confidentiality.

So, after identification comes authentication. Or in other words, only if you have valid identities, authentication will work. Now, suppose you go for your passport or suppose you go for getting a SIM card for your mobile services, you want to have a new SIM card, you go to Airtel. So there is any service provider not Airtel, it could be Jio, anyone. So they have a need by government regulations to identify you as to who you are.

So there is an identification process. So there in Airtel, you cannot produce your IIT ID card. That is not a valid ID . A valid ID is to prove that you are a citizen of India. And you have a unique ID, identification ID or number provided by the government of India.

That is the sort of identification they require to give you a telecom service. And therefore, you may go and claim in a telecommunication service provider's office that I am Saji, please give me a SIM card. And so and so are my credentials. Well, you claim to be Saji, you claim to be a citizen of India, we want to verify that. We want to authenticate, who you claim to be.

We want to verify. So authentication is nothing but verification. So you come to the IIT gate and say I am a student of IIT Madras. Well, give evidence. So your ID card serve us a source of your authentication.

It is already created, identification is done, you have the ID card. For authentication, you produce your ID card. In a passport office or in telecom service and related services, they ask you to place your fingerprints. There is a fingerprint reading device where they ask you to place your fingers. What are they doing? They are doing authentication.

Because in my Aadhaar ID, I have shared my biometric data. Biometric data is stored in the Aadhaar database. And when I claim that I am X, let us check whether you are X. X's credentials is what actually is already stored. So as X, I am giving my credentials.

If the credentials of my biometric matches with the credentials which are stored against X in the Aadhaar database, your authentication is done. You are, you claim to be X and you are actually X, we verified. Authentication is nothing but the verification of ensuring a person is who he or she claims to be. That authentication is the entry, the gateway or the entry into a computing system or an organization. Once authentication is done, you are allowed, you are inside.

You get the point, you showed your ID card, you are in. But you have to create the ID card, that is identification. Authentication is, well, verification. Whenever there is a need to access resources, you need to show that identity and then there is an authentication process. You try to access your Gmail or your Yahoo mail or your IIT mail.

What do you do basically? There are two fields there. One is, you write your user ID. What is that? Saji@iitm.

ac.in. That is my email ID. Well, fine. That is what I claim to be myself. But it could be you tomorrow, want to see my emails, what is going on, between someone or somebody, you know, you have something in the email which you want to see. You can claim to be me. So therefore, there is authentication.

Well, you claim to be Saji, fine. So, tell me your password. So, password is, you can say another, biometric is one, you can say, password is one of the long standing methods of authentication. You basically disclose something which only I am supposed to know. This is something I know, you know, biometric is something I have, password is something I know and only I am supposed to know.

That is the secrecy of password. When I enter my password, the system will cross check whether the password is correct and then you are authenticated. Essentially, password is also a method for authentication, whether you are me or you are somebody else. And if of course, my password has leaked, of course, you can become me. So that is, that is a weakness and therefore, you have multi factor authentication today, We will discuss that later. So, authentication based on the criticality of services that you are actually signing into, is a very, very important step in cybersecurity - identification, then authentication.

And the third important word is authorization. All these three are together key concepts, for particularly, for confidentiality - identification, authentication and then comes authorization. Authorization is about defining the level of access, what you can access and what you cannot access. Suppose you enter IIT campus as a student, as a student, you have certain privileges. For example, you are allotted a hostel room, you can straight away go to your hostel room and enter the hostel room, you are allowed, but you cannot enter a faculty room, that is not allowed.

So, therefore, there are certain privileges, when it comes to databases, or say Moodle, look at Moodle, which we use for our course management. There is a student login, there is a faculty login. So the authority, level of authority to access information is limited for different roles. And that is known as authorization. So a system based on your, after your authentication, provides access to resources based on your access rights.

And if authorization is to be done effectively, then the access rights have also need to be defined properly. So who is who, what are the different roles and what are their rights to access etc, need to be predefined. So in summary, you can imagine two aspects of cybersecurity or management or information security management. One is to classify information, information need to be classified and people also need to be classified. And then there has to be a mapping between people and information.

So, that actually decides the level of authority. So we will understand these concepts a little more in the upcoming sessions as to how to do an information classification, what are some of the standard practices available, say in industry, in military, and so on. And also how people are classified, in terms of their roles. We will get into those details later, but at a fundamental level, these are three key concepts. Do you have any questions here? Otherwise I move on to explain a couple of items more and maybe you will be able to relate to these concepts in the case that we are going to discuss.

What went wrong? When we look at certain instances, you can see where was the problem, was it with identification, authentication, authorization, or was it with accountability? So accountability is related to incidents. For example, suppose there is an incident in the campus, someone entered the campus who is not supposed to enter the campus and created a problem or someone entered the ladies hostel in the night, who is not a student, who is not a faculty, who is not a staff, then that person had no authority at all. There is a problem of authentication. The person who is not supposed to enter, entered or got access to systems. Now, what action to take? There comes the problem of accountability.

If something goes wrong, who is to be held responsible? Who was, for example, in our general security scenario, who was the person in the security, in the security post? Was that person sleeping? Or how did that person get in? So therefore, who is responsible for cyber security breaches or incidents need to be ascertained for taking actions, simply for taking actions in the case of incidents. That is known as accountability. That is where any data breach, who accessed and how that person got access, should get assigned to someone, some role. Again, we will illustrate that using case studies, as to how this accountability can be fixed. If nobody takes responsibility, then it will happen again.

And you do not know. And what was the vulnerability? And that is something which a administration should take action upon. And therefore, sign in and log data, which are to be maintained strictly in organization is based on the principle of accountability. Keeping logs and keeping complete history of who signed in and who signed out into systems need to be maintained, for the purpose of accountability. What we do now in the next 15 to 20 minutes, we will actually discuss the case that was shared with you reading R3, which pertains to a major incident in the world of cyber security.

Okay. I would say this is major, because this particular incident had implications for industry and government, because government is also responsible for welfare of people. And when major incidents happen, that affects large number of people, it could be due to absence of or not having proper regulations, proper laws and law enforcement in the country. So therefore, government also comes into picture and this is one such incident, which was discussed world over. So, we will look at this case of Target corporation. And we will ask three questions, which are given here.

One is to start with, identify technological and managerial vulnerabilities that led to data breach at Target. This was reading R4 earlier, that is why the slide is showing it, but it is actually R3, Okay. Yeah, so, first question, so who wants to answer the question? So, I would leave it to you, you can, somebody can actually give introduction to the case, just summarize the case as a whole without, you know, giving any solutions or without doing a why why analysis or why this happened, but what happened is something that we can start with. And then we can look at why.

So anyone can actually answer. So what is this case about, what happened actually? We can see that Target has to, for maintaining their payment systems on the day of, we can say, the period of Thanksgiving 2013. The problem occurred when Target outsourced or we can say, gave the responsibility to a third party, like a Faisal Mechanical Services, which are supposed to control their climate services but due to some, it made hackers, it gave access to the payment systems, which leaked the customers information, payment information, such as credit card information and various information to the hackers, which they commoditized. So what do you know about Target corporation? Where is this company based and what do they do? Target? It's a retail chain based out of the US. This is the retail chain based out of the US. Target and Walmart are close competitors in the North America and they are into retail.

So and retail is a great business in the US, great experience and that's where people go. And what is the season, when this incident occurs? Christmas and Thanksgiving. So, looks like this is pre planned, right? Some hacker has pre planned to really hurt and harm the company, when the company is actually looking forward to a huge sale during the Christmas time. You want to add something to the case? Yeah. Just want to add sir, actually implementing , in a data protection system is a different aspect and actually following and actually knowing about that data protection system is another aspect.

Like, they had all the multiple firewalls and all the data protection system and all the other safety measures like automatic, you know, deletion of the malware and malicious. But then that function was off in this particular case and the employees were not trained or not aware about that thing. Okay. So, invest, you are saying, in other words, investing in cyber security technologies is one, but practicing is something different.

Okay. That is what you are actually trying to say. So yeah, so the case in point Target corporation, United States, Thanksgiving, Christmas period and when sales is at peak, there comes major report or a report a headline in the newspapers that, data breach. And that puts the company into a sort of big embarrassment and major crisis, a major crisis at peak time of sale. Now that is the incident, that is what happened. And this happened, of course, I think 2016 is, 2013- 2013 is the year when it happened. And you can see there are several case studies written on this, not just the article I shared with you because it is very important dominant data breach.

So let us look at the first question. We say vulnerabilities. Every hacker exploit vulnerabilities. These terms, exploit and vulnerabilities are technical terms related to cybersecurity. For example, we are conducting this class in this room.

And this class is meant for participants of this course. And the room is not locked. The room is not locked. That is a vulnerability. That is a vulnerability.

But not everyone outside is interested to come in. And suppose somebody wants to disrupt the class, somebody can come in. But when somebody passes through the outside, one notices that the door is closed and one may not enter in. But if somebody knows the door is not locked, the hacker is exploiting that particular vulnerability. Somebody who knows what is the vulnerability, exploit it.

So that is called an exploit. The exploit here, not all vulnerabilities may not be exploited. But there is, there are certain exploits here in this particular case. So, I am asking you to identify the technological as well as the managerial vulnerabilities. Can you think of, can you classify them into two? Yeah. So in this case, the information on the credit card data was stored at the POS terminal.

But even captured in that. Even the data transmission to the centralized systems of the company was encrypted. But the terminal itself stored data without encryption and it was accessible to anyone. So that was a technology vulnerability point. And at the same time, the managerial part of it was that the IT system had disabled some of the security measures or ignored the warnings that the system was supposed to do.

So you have gone to the managerial issue. So if you stay on to the technical part, one vulnerability was data that is POS data captured, including the credit card information within the POS system or the computer, where the billing is done. In the RAM, in the memory of that computer, it is not encrypted. When it is transmitted from the computer to a server, transmission is encrypted, but within the system, it is not encrypted. That is a technological vulnerability.

Is there any other, that is very good point. Is there any other technical vulnerability? The team has shut down the, like they turned off the malware detection software. Malware detection software, they turned it off. So they could not detect anything with it. Malware detection software was turned off because they wanted to receive emails and other internet access.

So they have turned it off. So what kind of malware detection software they had? Was there updated or was there really up to date or it was like, They were used to do that - internal and external assessment. So it was up to date, but they, because it was turned off, they could not know whether it was injected or not. Yeah. So, but you have entered the second aspect.

If somebody turned off, then it is a human failure. One more technological aspect, which is there is that, they allowed the third party vendors to their payment system or they should have limited the access towards it and that is what caused the vulnerability. So that is actually a problem of access. The vendor had access to the POS and what vendor, what was vendor's role or the third party's role here? It was a vendor for actually infrastructure maintenance or climate control, basically doing infrastructure maintenance and that vendor should not have access to POS data. So,there was actually a problem with the configuration, which is a technical error again, which is a technical problem, but is it a technical problem or managerial problem? It is a problem with configuration.

It is difficult to put it into one bucket. It is a technical problem. It is also a oversight or somebody did not pay attention there. So it could be an error. It may not be by deliberate action, but it is an error. It is a technical issue, but a management issue as well, a configuration issue. So where does this fall? Is it identification issue? Is it authentication issue or is it authorization issue? It is an authorization issue.

It is an authorization issue. That vendor had no authority to access that. So authorization was not clearly configured. So then we are getting into both. So I asked you to identify technological issues, but then you see that both are sort of so much tied together. You know, it is difficult to say it is a technical issue alone when human actors or human roles are involved.

So therefore there is interplay between the two. But purely from an administrative perspective, what would you articulate as the reasons for the breach? Pure administrative failure. They have, did they have audit, audit processes? What does the case say? They had multiple systems like we had multiple firewalls and intrusion detection and more detection practices. They had intrusion detection systems. They have malware detection and reporting, not just detection alone, but reporting as well. But they due to many false positives like in the various emails, they have received hundreds of emails per day.

So like, there was also provision of deleting the malware as soon as the system detected it, but they turned it off, citing many false positives. Well, that is a very interesting point. What are false positives in malware detection? And what is its role in the configuration of malware? You just found that somebody turned off the malware detection software. There is some reason, simply people do not do these things.

There is some reason why people do this. And the reason is what he is trying to articulate. Can someone explain it more, further as to what is false positive in alarms? In every alarm and detection, there can be false positives and false negatives also. And yes, you understand. The objective of the malware is to identify malicious software or installation, but sometimes it may highlight something which is genuine, which is correct information as incorrect.

That is true positive. That is true positive and it may hamper. That is the role of the system. That may hamper the day to day operations. False negative would be that someone who is not authorized access of software, which is not authorized access, is given access to the information and carry out some malicious activity. So that would be a case of false negative. So because, but false positives impact the day to day operations in some way, the tendency is to switch them off, if it is highlighting too many things as malicious.

False negative is very dangerous because somebody is actually a miscreant, but identified as not a miscreant. So that is a problem. But if you do not have malware protection, so everyone is in.

So that is a problem. So there are you can see there are multiple levels of protection. One is by configuration, you assign authority. And if in authorization there is a problem, then the malware detection sort of monitoring systems must be able to report that. But here multiple failures, a series of failures. One is authorization issue.

Second is, the next layer also did not work because you simply switched it off. And you switched it off because of false positives, meaning that someone who is someone or something which is not actually a problem, but doubted as a problem, is highlighted. And suppose these reports come every hour or there is an alarm that is happening every hour and many of those alarms are actually false alarms. Actually there was no issue.

There was only a doubt. Then, what happens is the efficiency of operations get affected. You, this smooth operation becomes a problem. So every time there is a likely malware that is reported and the system is stalled, then you know, people are standing in the queue. So you can imagine someone who is operating the POS, you know, the system stops because of malware, imagine. Then it is affecting the smooth operation of the, of the retail outlet.

So the complaint goes to the IT department. The IT department will say, well, there is no problem, we are clearing it. But this, if this becomes frequent during operations, it affects the efficiency. So one conflict here is, the conflict between efficiency and security. When you implement very tight security, there may be a trade-off with efficiency.

And that trade-off is something that needs to be understood. There are other instances of trade-off which we will discuss later. But cyber security systems may affect the efficient operations. And there the easy shortcut is,well, switch it off. Just keep going.

So bypassing is immediate step that sometimes engineers tend to do in planned operations as well. Yeah. So like this false posting and false entries are just actually like the type 1 and type 2 errors. And actually no system can be 100 percent reliable or 100 percent, you know, precise.

And just bypassing is just like removing the filter. Then, that filter is not there. So filter has to serve its purpose actually. So that actually, we will talk about solutions later. What should have been done or what should the company do is an important thing. But people in order to address the loss of efficiency tend to bypass security or safety measures.

We can relate security with safety. Bypassing it is the easiest. And you see that was actually done. And what do you think about the log, the login, sorry, the log files. Was there complete logging done or logging was not complete. Is there any mention in this case, about it? So that is another thing which engineers try to do because if there is complete logging of processes, system can again become inefficient. So they try to do that. So these are some of the bypass that managers tend to do or engineers or technical people try to do to address the problem of efficiency.

So there are technical issues. There are managerial issues. It is a combination of both which led to this particular incident.