**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: 15**

Good afternoon all. Today we, members of group 3 are going to present an article that was published on HBR, which is based on internet insecurity. This article basically discusses a new approach apart from the traditional approach, a new approach how we can prevent cyber attacks, a new approach of cyber defence apart from spending on cyber intensive resources. So we will first present our key statistics that says that there has been a growing trend of increasing cyber attack over the years. It shows that in many areas like USA, North America, Latin America as compared to 2021 there has been a certain jump in cyber attacks in 2022 and the most attacked industries in 2022 has been government sectors, healthcare sector, education sector and specifically critical infrastructures. The global volume of cyber attacks in Q4 in the year 2022 has been an average, on an average basis, weekly it has been 1168, which is really a staggering figure.

So the question that the article asks is whether investing in latest cyber defence guarantee a success in preventing malware attacks and it argues that no amount of spending on defences will actually, can actually protect us or guarantees that it will shield us from cyber attacks and so it introduces to us a new approach and over the, over our presentation over the course of our presentation, we will see what will be the new approach. So as we see that over the years starting from 2021 there has been an increase in global cyber security spending. By 2025, it is projected to touch 460 billion dollars and over the years it has been increasing at an average rate of 15%. This research was done by Kasper Sky, which revealed that in the year 2022 the expenditure on cyber resources is going to exceed the 300 billion dollar mark and the cumulative spending from 2021 to 2025 is going to touch 1.

5 trillion dollar. So now let us focus, what are critical infrastructures, what are the sectors that come under critical infrastructures and how they are becoming more and more complex over the years. Now the energy sector, the power generating plants, the telecommunication sector, some manufacturing sector which are critical, apart from the transportation sector, water treatments, all these come under critical infrastructures. Now let us see why the complexity is growing. Earlier all these sectors were decoupled, they were not dependent upon each other but due to over dependence on power, maybe even in the transportation sector we have battery driven, so for charging these battery driven vehicles we need charging stations which are connected to the grid as an example.

Even the telecommunication sector is being related, being connected with the energy generating units, smart grids and all. So this has been, this all this critical infrastructure like generation distribution is becoming more complex because they are now a network of connected device, They are forming a grid. So even if one of the critical infrastructure fails that can lead to a devastating chain reaction and the entire system can fail. Some of the news articles that we found, like regarding the cyber attacks that has happened over the years on critical infrastructure specifically in Saudi on Saudi Aramco, then some nuclear attacks on South Korean nuclear plant. Again the Chinese are targeting our Indian power grid, they are developing some malware named as RedEcho, Ukrainian power grid was also attacked.

So we will see some of them. An example can be Saudi Aramco, which is one of the largest oil generating companies in Saudi Arabia and from 2012 itself there has been multiple attacks, like in 2012 there has been one phenomena, one virus name as Shamoon that stole all the passwords that attacked specifically more than 35000 systems, wiped entire data, stole passwords and even they prevented the computers from rebooting. There was a lot of outage in the system and even the system took 2 to 3 weeks to restart. So there was a lot of financial impact. Apart from that even in the 2017, a malicious software attack happened which targeted the safety controller system.

The safety system was compromised and it stopped working so it led to an entire shutdown of the system. Again in the 2021, in July what happened that again, it fell victim to an extortionist attempt where the data, sensitive data of the company got leaked by one of their third party contractors and the hackers demanded a whopping 50 million dollar to get the data deleted. Now apart from this refineries and all, we see that the power grids that are also facing some cyber attacks, sophisticated cyber attacks. Recently, on April 2022, when the Russia Ukraine war was going on, the Ukrainian government said that it just had a narrow escape from the cyber attack which was led by the Russian agencies, Russian spy agencies where they targeted some of the largest energy generating companies of Ukraine and they tried to trigger a blackout by stopping the grids and it was done, it was the effort was done or the intention was to, you know, if you induce a blackout, the invasion would have been softer and easier. So obviously they were lucky to escape.

So now coming to the fact that there is a tradeoff of capability versus vulnerability when the digital transformation is considered. As we have seen that in the industrial control system there is a rapid digitalization application of IOT, AI-ML, Cloud technologies have made the decision making entirely very fast and efficient and in the age of high end companies it has become really indispensable all these technologies and nowadays the industries are also dealing with terabytes of data on a regular basis, so this is making the

entire system very fragile. As we know data is a new one, so all the decision making everything is being driven by the data and that is why there are many vulnerabilities that we need to address. Now the next part will be addressed by my friend where the growing vulnerabilities and the techniques that we need to devise to deal with those things, will be discussed by my friend Lokesh. Thank you, Sir.

Now the thing is, does fast pace of digital transformation requires increased security ? Why now, the question comes? Because nowadays the use of digital transformation and their growth is more. There could be many reasons and COVID is also one of the reason and that digital transformation is happening at a faster pace. Whatever may be the company, whether it is an organization or industry they are moving towards more, towards digital aspects so that they could remain in the competition, so that they could get better and effective decisions and employees need modern tools to be effective. The things means we could see automation, IoT, cloud computing they are using, organizations are using extensive, but the thing is, so we are moving more towards digital aspects. So does it requires, the question is does it requires more increased cyber security or will the reliance on cyber security got reduced? Now the question is.

But when we got into facts, it gives the result that as we are go as the digital transformation is happening at a faster pace, vulnerabilities are also growing. For example, we are using a complex hardware, you know the technologies are coming so that complex hardware and software tools are using. So in order to enhance the capabilities in the same way, vulnerabilities are also increasing at the same rate. For example, vendors even also do not know what they are, means what are the vulnerabilities associated with the design of new hardware and software tools. When they are exploited means, when they are attacked by some threats they are getting, you know, for example information systems of the US companies they even, they are using some advanced information systems, so in order to detect the threat itself, they are taking more than 200 day, 200 days on an average.

In some of the cases, they are being notified by some third parties. Here the issue is, every company or organization looking for fast and better solutions, reduction of human errors and reducing the cost. But the thing is they are welcoming the other end of risk, like cyber risk means they are investing in new technologies, reducing the cost of employees, labor cost, everything dependence on the human and everything. But again they are investing in returns in cyber security means again they are driving up the cost. This is happening with the invention of, means with the fast growing of digital transformation.

So what else could be done, means when there are any problems, we will implement some checks some proper checks in order to handle such situations. One is hygiene.

Hygiene means generally we suppose people , some people used to go to doctor in order to regularly check their health and during COVID times we used to sanitize very frequently. All these things we used to do in order to protect ourselves from the disease. In the same way we have a concept called cyber hygiene where the organizations or the companies use in order to check the security of data, users, networks, everything.

But these are some benefits but the, how it is assessed means there is an advanced performance monitoring solution that can scan the entire IT environment of a company. So it will scan means what are the assets available, what are the vulnerabilities associated with that assets, and it will provide a performance scorecard whether it is critical or low, medium or high. Why we are doing these things is, just to keep the bar against the hacker or the threat so that they could not peep into the company's network or the organisation network Some of the regular approaches of cyber hygiene is deploying the latest software and hardware tools, regularly training the employees in order to avoid and inspect the issues and also separating the important information systems from the other networks. Some of the practices at the organization level, from an IT perspective if we means generally we have to change the passwords every month and it should be very complex and means we cannot use the password in a simple manner, it should contain special characters, like that, if we talk with respect to the passwords and installing new security patches periodically and if we, there are zones everything means, we cannot get access to entire means, every aspect in an organization. It got limited to only some of the users but doing so means investing millions of rupees but millions of amount, it does not solve the problem because nowadays hackers are more, they are more conscious and a targeted we cannot escape from a targeted attack that is one of the reason.

Another reason is we cannot create comprehensive inventory of the company's hardware and software assets, in case of asset intensive industries such as a transportation, energy etc. And one more limitation is, if there are suppose, if we consider a large power station there are more substations, they are widely dispersed, in such cases if we are rolling down any upgrades in one system, suppose if there is a, if the hacker got into, entered into that network then it as said by Sayan, entire grid can be collapsed at a time, that that could also be a possibility. So after seeing all these limitations, we can see that how much you invest in technology or in resources everything, we cannot avoid the attacks. So the only means, one of the solution that, that is available is reducing the dependency on digital aspects, means moving away from digital aspects to some other means, some sensitive systems we can completely reduce the reliance on the digital aspects, that that can be explained in the next slides by Vijay. So we get back to the article in question and this article, HBR article was written by actually Andrew Bochman and basically from the headline of the title itself it goes in a different direction it says that it is not cyber security, it is cyber insecurity.

So as previously explained by Sayan and Lokesh that the aim is that, ultimately that you have to reduce your dependence upon the digital platforms and anything which is connected to the internet. So in, towards this idea now this gentleman Andrew Bochman or in short he is called Andy, now this guy works in the Idaho National Laboratory and at the Idaho National Laboratory came up with a novel concept and they have been working on it for a few years now and this different approach was that they said that firstly you identify the most essential, the critical functions as which is likely to jeopardize the entire operation of whichever sector one is in. You reduce and eliminate the digital pathways which any attacker or any threat which is there, so you reduce those pathways, you can not totally eliminate them but you reduce as much as possible and you shift away from full reliance on the digital connectivity and keep contingency plans or build redundancy in that, so that you the critical function continue, even if there is a attack. So now this was the Idaho National Labs stepwise concept approach they basically devised two basically frameworks the first framework they called as Consequence Driven Cyber Informed Engineering or CCE in short and the other was a companion framework which was developed which is called the Cyber Informed Engineering. So the difference was, the Consequence Driven and the other was Cyber Informed Engineering.

Now though broadly, they are both the same but the level that which they have been perceived to that they will deal, is different, which I shall be explain in subsequent slides and as you can see on the view file that Andrew Bochman has been working in the INL laboratories in here he is a senior grid strategist and they published a number of books and this particular article refers to the book which is being shown on the view file. He is, he has been providing guidance to not only US government but other governments and industry leaders also. He is a ex-Airforce personnel and he was working in IBM and other known companies also. So moving on, so just a short definition about the Cyber Informed Engineering and the Consequence Driven Cyber Informed Engineering. So the Consequence Driven Cyber Informed Engineering developed by the Idaho laboratories the basic objective was that they wanted that the hierarchy should have a change in the perception as they view cyber threat, not as a cyber security but rather see it as a cyber insecurity.

No system which is connected to the digital platform is secure, no matter how many firewalls we build, no matter what our protection detection system. So the aim was to build in redundancy that even if there is an attack if your critical functions continue to function in the way they are supposed to. So how do we do that? So we will come to that, the next framework associated with that at a slightly lower level is the Cyber Informed Engineering. So the difference being the Consequence Driven and this was a companion framework developed by the same laboratories, as I said it is similar to the Consequence

Driven Informed Engineering in many respects. The objective over here was that when a system is being designed especially in the industrial digital platforms, the cyber risk mitigation factors or aspects should be integrated right from the conceptual stage itself.

Now we design a boiler or a big platform thereafter it is connected to the digital grade controlling system thereafter we think about securing it with various cyber assets. But the CCE says, as an engineer, when we think, when we conceptualize something is required some problem needs solving, try to figure the cyber aspect beforehand only in the concept in the design phase and in the production phase itself. So that it saves a lot of time and it is much better secured and the redundancy is built in when it is brought online in any domain. So from the engineers perspective, this was a challenge because you have to understand the impact of cyber attacks across the entire product or the program life cycle of whatever you are building. And as the cyber threats, they keep on evolving, they impact the design, the development, deployment or the program life cycle of whatever and operational phases of all stages of a system it can affect at any stage.

So wherever you find the loop, the cyber threat might manifest itself. So the CCE and the CIE processes basically teach to heed and incorporate the cyber security aspect right from the beginning itself. It basically says that you start incorporating the cyber aspect from the engineering perspective right at the conceptual stage itself and that no system is safe. It is not saying that you do away with automation, it says that you build in redundancies you take care of the threat aspect well before and have contingency planning or continuity planning or redundancy so that your critical functions continue to move on. Now this, the implementation as suggested by the INL laboratories as given in the article was that initially they were thinking that the CCE master plan they will be implemented by the INL personnel and thereafter subsequently by INL trained personnel across, through various service firms and the corporate hierarchy, it was aimed at the corporate hierarchy basically, the those who are responsible for the regulatory compliance litigation CEOs and CFOs and basically those critical supervisors or those people who are actually overseeing the critical operational functionalities in any industrial sector, the safety systems expert the operator, those who are going to be the first responders to any kind of malfunction or any issue which is there in the plant.

So the process was basically, the first process was a four step process as shown on the view file- the phase one was, as we said the critical word over here is the consequence driven. So the consequence driven is what is the ultimate the greatest loss or most critical function in my domain or my responsibility which is likely to jeopardize the entire setup or the entire business or the entire goal of my firm. So that basically that would be the consequence and that would be the priority in a CCE This should be targeted, that this should not shut down in the event of a cyber attack. So that becomes your consequence

prioritization. Now in order to do that, you carry out a system wide analysis.

In that system wide analysis, you are basically looking at what are the pathways which are coming to this, which may result in this particular consequence and from that you carry out, that okay, these are the pathways and how these pathways will be targeted, through what all means and through what all people, where would they be located. So you carry out analysis like that and finally once you have carried out an appraisal from the first step to the third step, you come to the final step that having based, that this is my consequence, these are the key system, key pathways from where they are going to attack and these are the kind of people or the targets which they would like to attack and they will be likely located over here they will be looking for this thing, you come to, then you come to the mitigation and the protection measures, which you would like to implement and that basically says that, get back to or at least incorporate some kind of analog or disconnect from the digitalization, not totally but as far as possible, so that you critical functions continue to move on. So as shown in the article the same processes, identify the Crown Jewel, that is the main function, you map the digital terrain through which the people are likely to approach you or carry out their threat and then you eliminate the likely attack paths through to reach that consequence by the cyber adversary and you generate the options or mitigation measures to thwart those actions. So these are the recommendations which are given in the article and the article suggests that firstly you need to learn to think from the adversaries point of view. So you have to take a very neutral view and think from the cyber attacker's point of view as to where they would like to attack your institution or firm or whichever domain you are in.

So for that, you have to wargame that scenario, you have to sit across the critical people, the people responsible for risk mitigation, the expert the supervisors and then you have to take an opinion from each one of them what do you think is the most critical in your domain, what do you think is the most critical and there it will lead you to a one main critical factor or few critical factors which are likely to jeopardize your company and there one you will get your consequence, your prioritization, you will get. So not withstandingly constantly high levels of cyber hygiene as was mentioned by Lokesh you can have all levels of cyber hygiene but when a determined attacker is there, as given in the article, no matter of what sort of security we take, it is only going to prevent those 10-15% of the attacks and a dedicated attacker who has got the resources will eventually get through your system, that is how the digital platforms work, there is vulnerability and there is also help also or the facility also but vulnerability also exists. So employees need to be aware, a cyber safety culture has to be there, and so that you are able to recognize whenever such a threat has started manifesting itself, which can manifest itself in any manner like a small glitch, a small trip somewhere, so that particular person who will be the first responder has to know okay, now it has started if you, if you do not do that, you

will reach that it will finally affect your critical system, then it might be too late and that is why this CCE is designed that even once that thing has happened you can go back to, you can go back to activating your redundancy or contingency which you had built in the system. So what kind of contingency planning, you have to support your critical functioning you have to war game and go on to what is my critical functions you have to maintain that continuity as we discussed as far as possible maintain a air gap network, especially from the internet and your redundant system, it should not happen that again is connected to the digital platform or to the internet. So you, one system has been attacked and your redundancy platforms are also being attacked so your contingency plan will fail over there only, so this aspect has to be looked at and thereafter the article says that, what is the requirement of this, basically because traditionally, when the engineering goes from the conceptual stage nobody pays much attention, the curriculum does not include the cyber aspects and the cyber aspects is an afterthought as we discussed before that people think about it at a later stage once everything has been installed okay, we will put a firewall, we will put an intrusion detection now that the thing has been connected, we will do, take all these things and now it will be secure but it does not work like that and engineers it says, that engineers know their job very well, they know that we are an engineer we have to weed out all these problems so that is there in the systems which they design, conceptualize design and produce but the cyber aspect also needs to be known by the engineers and when they are designing anything they should be made aware to incorporate this aspect also, as far as possible and why this is there is, because therefore there is as far as definition is concerned of this that the awareness of the security challenges in the operating digital and non-digital industries is very less and the INL says that this is a philosophy and not some kind of step by step process, so it is a philosophy that everyone must imbibe, that this cyber aspects have to be taken care of well at the conceptual stage itself and their objective they say that is the promulgation of a strategy to learn and view cyber like any other modes of failure it is also a mode of failure which an engineer, while designing the system should say, there are many other modes of failure but he should also figure that cyber attack is also or can also be one of the modes of failure and I should figure it in my plans well in advance.

So this initially as I was telling that, the main difference between the consequence driven and the cyber informed engineering, if you see the second part they are both the same so what makes it different, what makes it different is, if you see to the left top of the slide, the consequence driven basically is carried out at a very higher level, that is the national security level events by a well organized state sponsored or person people with lot of resources and all, at a lower stage, cyber physical attacks or targeted IS attacks is what the cyber informed engineering says that it will deal with at a higher level, at a more broader level it is the Consequence Driven Cyber Informed Engineering which says that it has been designed to take care of those kind of threats. So to conclude, as the article

says that these are the things which we must keep in mind, cyber attack vulnerability, all organizations which are dependent on digital technologies are vulnerable to an attack and can be attacked, may be attacked and cyber adversaries are highly skilled and it is a field or it is a domain wherein they are keeping, they are more updating themselves rapidly. So you need to catch up. The strategy is, as far as this article and INL says as brought out in the video also, they are saying that take a step backward, we are not saying that completely shut down, take a step backward and backward in the sense, incorporate analog technology so that you are away from what has affected you, that is the digital platform as far as possible Continuity and survivability should be the goal of the firm and that is how we should look at it, when we talk about Cyber Informed Engineering. Yes, cost wise an analysis should be there and management has to be there and as brought out over there, higher cost initially but the potentially devastating price of business as usual, it can lead to disastrous consequences and for a penny, a pound might be lost, so well in advance all these concepts, these thought processes should be incorporated by the people responsible or looking after the respective domains.

That is all from our group over here. Thank you for the presentation. So it gives us an introduction to the cyber security concerns in the modern era where the author said that any system that is connected to the internet is not secure. So this is a very disturbing statement and we have a case which is a sequel to what is discussed. So in that context we will take this idea forward. Protecting the shader, that is the next case which is a sequel to this so we will look at it from a more practical point of view and that is in the next class. Thank you very much.