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: 03
Lecture: 07

Hello and good morning, welcome back to this course, Cyber security and Privacy - third session. So today's topic is Governance, Risk and Compliance or in short, this is known as GRC. GRC is a common terminology in cybersecurity circles. So we will get introduced to this broad framework, this broad management and governance framework. As we saw in the previous sessions, this course is about cyber security management, not cyber security technology. So technology is a constituent, but we are looking at how organizations can manage cyber assets effectively.

So it is a, we are looking at it as a management issue. And when it comes to management, you are already aware, most of you are students of management, we know that we talk about standards and frameworks and, you know, more systematic way or more efficient way of addressing issues in manage, management or management is about managing resources or cyber assets are resources to be managed by organizations. So as we go, we look at what these concepts really mean, like what is Governance, what is Risk and what is Compliance? So of course, the item in the middle, that is risk, is something that we are going to elaborate further in the subsequent sessions because cyber security is a source of risk or cyber threats are sources of risk for organizations and they need to be managed. So we need to develop much clearer understanding about risk management in the context of cyber assets.

So that is our plan for today. We will discuss broad frameworks, we are not going to get into the details of how, what they constitute and how, for example, how they can be assessed or measured and how they can be controlled etc, which will come in the subsequent sessions. Alright, starting where we stopped in the previous sessions, we already are aware that the world is digital today or a lot of things that we do today is related to or through digital technologies. We have a bright side and also we have a dark side, which is the cyber threats. So good people and bad people are the positive views and the negative views of technology.

And we can see organizations have been victims of cyber attacks in the past. And we may think that with advancement of technology, cyber threats would cease to exist, but unfortunately that is not the case. So the volume, the cyber incidents in terms of volume and in terms of impact, in terms of impact are growing. So you can see the most recent

data breach, which I have shown in this graph is of Marriott. So this was in 2019 December, there are incidents after that, but this is what I am showing.

So you can see the number of people affected, it is 500 million. So 500 million data records were compromised in the sense, unauthorized access by hackers or external people who are not supposed to access that, could access the private data stored in the database of the Marriott hotel chain. Who knows, if you stayed in Westin and you actually shared your credit card details or you booked online, it may be out in the dark world for sale. So that is the sort of vulnerability that you feel, you know, Air India's data breach, you immediately fear, well, you have booked airplanes online and using your credit card and who knows whether you saved it or not, you may have forgotten or your credit card details, it is fine, but for efficient online activities, you generally save your credit card, you may have your credit card details saved in Amazon. I am not threatening you, if Amazon's data breach happens, you know, all of us will be in a soup including me.

So that is the world. So it is, it has not stopped, but it is only going up. And therefore, we discussed Target stores data breach, which is also shown here is much smaller in terms of its extent but you can see this is growing. And therefore, organizations, these are major attacks on organizations. It is like thieves entering the premises of an organization and stealing away assets.

So and therefore, just like there is physical security, there has to be cyber security to protect your cyber assets. So that is the premise. Well, you can wish everything well and live on, but the future will be bright and future will be good and there is God above watching over everything. So all that is good thinking, to calm down your mind. But you know that as managers, you will always wish for the best, but prepare for the worst.

That is what we say. So, fortune favors the prepared mind, is a very famous quote by Louis Pasteur. And you know what it means, you can leave things to chance, but because oftentimes future is unpredictable, you can not actually predict, but how prepared are you for an unpredictable future? So have you thought through, what could go wrong? Have you accepted that things could go wrong and how prepared are you ? So one thing is to say that nothing is predictable and you know, so whatever we do, still things can go wrong etc. and take a stance, well, do nothing. The other is well, things can go wrong, but we may not be able to do.

So that is Louis Pasteur, be prepared, be prepared and be prepared. So that is the message. So broadly, there are three approaches to cyber security management. From a higher level, I would say if you look at cyber security management from a broad perspective or you stand in front of an organization and then think in broader terms, what are the different

approaches that one could take to manage cyber assets? Then, I would figure three approaches. These are not given exactly in your textbook as it is, but I am actually referring to multiple sources to build these three categories.

So the first approach is the GRC approach, which we are actually dealing with today, which is very popular, which is the framework based approach. So in this, you can actually think of the, in the first method, which is GRC, you are looking at cyber security and cyber security management as one among the many risk management initiatives, you need to have in an organization or cyber security is a part of the risk management framework of an organization. There are other risks that an organization needs to manage and the cyber is one. For example, there is operations risk, there is market risk and so many other risks that constantly affect organizations. Therefore you function in an environment and therefore, there are internal and external threats and organization faces.

One category is the cyber related risk. But when it comes to risk management, you do not look at cyber security alone, you make it a part of a overall enterprise risk management framework or also known as ERM, we will come to it in the next slides. So cyber security as a part of the overall governance, risk management and compliance with law, compliance with regulations, compliance with internal and external standards. That is one broad approach to, I would say, the broadest approach to cyber security management, you do not look at it as an independent constituent, but you actually manage it as a part of something else, a bigger initiative. The second approach is the standards driven approach.

Standards driven approach looks at cyber security as a separate issue or a separate category and it is distinct from other risk that an organization faces maybe or you may actually be, it may also depend on the size of the organization and the nature of the organization etc. For example, a small organization, a medium sized organization may not have GRC framework or larger frameworks in place, but they would still need to address cyber security. So one way of addressing cyber security in a standard way is to implement a cyber security standard, which is defined by standard bodies like the ISO or the NIST. NIST is an American standard body and ISO is European. So they have defined standards for managing cyber security.

So when you implement the standard with the help of a consultant, you actually are implementing certain practices or certain practices that would ensure that your cyber assets are protected. So that is, I would look at the standards driven approach as a distinct approach or different from the GRC approach because you are focusing on cyber security alone. But there could be cases where a standard is adopted as part of the GRC framework as well, that can also happen. If you know depending on, I said the size of the organization or how big you are and what, how much of cyber assets you have etc. would determine

how you go, but these can exist independently, this can exist together as well.

That is the point I am making. And the third approach, I would call it the textbook approach. And that is what you are going to learn. So if you actually go by GRC, ISO etc. you should go for training.

Because standard training is available in the market to get trained say on ISO, IEC 27001 or some of the standards in GRC, which we are going to see, there are standard training modules available. So that actually helps you to do things in an organization. But our approach here in this course, this is education or training. And therefore, to help you understand various concepts related to cyber security management. So in your textbook, you would see there is an organizational planning approach which they have suggested.

So many of the practices that are under GRC or under the ISO are covered actually in a, in the textbook, but not necessarily complying with any of the standard frameworks or standards that exist. So in the organizational planning approach, cyber security is presented as something that should be prioritized in the strategic planning of organization. So there should be a priority at a strategic level, at a higher level. So cyber security is not just something that should be considered at the operational level, but it should be at the strategic level. And contingency planning is a constituent of the organizational planning approach.

So there is strategic planning, there is also contingency planning. And so both this put together actually addresses cyber risk. So that is the perspective or the view that in an academic course that we take. And this could be implemented as standards or frameworks differently. You might be aware that there was a major cyber attack on banking institutions some years ago in India.

I guess 2016, when credit cards, sorry, debit cards became vulnerable. And following that the Reserve Bank of India made cyber security as a strategic initiative mandatory for banks. So this has to exist separate from the IT management. So there used to be IT department, IT head and so on in all banks. But RBI has made cyber security management a strategic part of banks today with that incident.

Of course all of us today have the chip based cards. That is another thing that RBI made mandatory for all banks. So, there are structures that regulatory bodies would insist on certain domains of business. And then you have no option that you have to treat cyber security as a priority. But that may not be the case, say with certain other domains like education.

There is no mandate that we should have a CSO and also a chief security officer or chief information security officer. We do not have one because there is no regulatory body insisting that. So this could vary from organization to organization as to how much you invest in compliance or how much you invest in cyber security. GRC may be a mandatory requirement, compliance may be a mandatory requirement. Then you, your business is global and you have to work with organizations which insist or partners, business partners who insist on such kind of frameworks.

So now, coming to the next level to understand GRC approach that is governance, risk and compliance approach. There are again three broad approaches. But before that, let me ask you this question what is, what do you mean by governance? You hear these terms governance and management. So here the word is governance and not management. So there is a government for a country.

And then of course, there is central government and there are federal governments and there are local governments and there is a government within the organization or within the subgroup where we belong to - functional aspects of rules and regulations that are. Rules and regulations. Yeah, emergency response. So that is very much specific to cyber security. But governance as a term, is a higher order term than management.

So generally, we know that there is a governing body for organizations. There is a board for organizations. So the governing body's role is to institute a management or management structures, management procedures and also monitor them. So there is a governing body means a governing body is an overarching body. There is a higher body which is continuously monitoring the health of an organization.

They have placed management systems in place. So for example, the CEO is actually chosen or selected by the governing board. So they place management in place. So governance is the higher body which is responsible for the overall organization. And of course, then of course , you have the C level executives and other management structures which actually makes the organization function and go in the direction it should go, set by the strategic priorities of the organization.

So governance when you actually bring the word governance to cyber security you are actually looking at cyber security as a strategy. So at a very higher level and it is having the highest priority as far as an organization is concerned. So that is the meaning or that is the implication, when you link cyber security with governance. So there were standards that were developed for governance of organizations in the 90s. Again, this is a topic we will touch upon later.

The Sarbanes Oxley Act or SOX as it is known as an accounting standard in the United States, was developed post major scandals that happened in the United States. Accounting scandals that happened in the United States. And such scandals can completely bankrupt an organization and a large organization like the Enron, if you have read about, could go bankrupt in a short time because of scandals. And that is a result of absence of governance. There is no body that is monitoring whether this organization is functioning healthy or not.

And if you do not have that supervision or that guardianship I would say, then the organization exists today but may just get vanished because of major scandals or major fraud as we call it. So and subsequently there was, of course compliance for accounting, compliance for managing its IT. So one of the jobs that was created for IT industry post the scandals, thanks to the scandals, is implementation of standards, particularly accounting standards and control standards for organizations because IT became a system that can actually help implement compliance in organization because you cannot manually monitor, manually check or manually report. These are actually very huge tasks and therefore IT systems came in place to implement control and compliance of standards like accounting standards in organization. So there are standards that were built by information systems community.

COBIT is an example. COBIT is a specification or is it a, it is a standard for GRC specified by ISACA, Information Systems Audit and Control Association. ISACA is a global body and if you want to get trained, I talked about GRC training or standards training, if you want to get trained on security, ISACA is one body and there is a local chapter always, Chennai has an ISACA local chapter. You can actually visit their sites and see what activities they do. So ISACA is the body which framed the COBIT standard control objectives of information related technology and COBIT framework provides for managing cyber security and it also provides for managing other aspects of risk in an organization or compliance in an organization. So this is Information Systems Audit and Control Organization.

So basically from an accounting perspective also, COBIT enables monitoring and control. So it puts in place control systems in one sense. So this is IT based control of organization.

So IT gets the priority here. So that is the root. The next framework is the COSO framework which is expanded as Committee of Sponsoring Organizations or COSO. COSO has a framework for GRC, framework for Enterprise Internal Controls. So it stresses on controls. The key term there is control, not risk. So I will show what are the areas where this COSO framework focuses on in terms of monitoring and control.

So it is a framework initiated by American Accounting Association or AAA. So this is a framework that is specified by an accounting body not an IT body. So COBIT is from an IT community, COSO is from accounting community. So there are, these are two basic frameworks and COSO got expanded as Enterprise Risk Management Framework or ERM. ERM is standard term in large organizations, ERM framework.

So you know, you talk to large international organizations they will talk about their ERM framework or ERM initiatives as to what they do. So bringing all risk under, as a risk that organization has to manage and cyber risk is one of them, as I pointed out in the beginning. So what ERM has done is, it has added certain specific clauses or specific elements to COSO. So it expanded COSO to make it a ERM framework, Enterprise Risk Management Framework. So from accounting and internal controls, COSO expanded to the larger enterprise, risk management of the larger enterprise and that is COSO ERM.

So this is risk based approach. So there are three broad frameworks when we look at GRC standard frameworks. So which are available in the industry for any organization to adopt one is COBIT, second is COSO and third is COSO ERM. So these are GRC frameworks that are available and there are actually industry bodies associated with each of them. So this is at the enterprise level not at a specific cyber security standard level like the ISO or NIST, wherein cyber security is a constituent of this framework. Now, we refer to internal controls, we said the COSO focuses on internal controls.

So what does this term internal control mean? So that is what I list here, for the purpose of understanding. And then of course, you can go to the next leveL, then you will see more details for each of this. But what does it try to control? So what are the control systems that are put in place in the form of processes and processes that needs to be controlled? So there are processes for safeguarding assets, processes for maintaining sufficient records, provide accurate and reliable information, prepare financial reports according to established criteria, promote and improve operational efficiency, encourage adherence with management policies, comply with laws and regulations. These are different aspects of controls.

So the control systems focuses on these areas. So this of course, breaks down into further details when it comes to implementation of the processes in the form of standards. So the internal controls work in three aspects. And again this is very intuitive. There are preventive controls which deter problems from occurring.

So it is futuristic or it is preventive in nature. There are detective controls. It is like you identify or you detect and then of course, do the firefighting. Those are known as detective

controls. And corrective controls, post detection how you actually do the course correction.

That is the corrective controls. You know, just like in any maintenance activity, you have similar terms like you have preventive maintenance, breakdown maintenance and corrective maintenance. So this is very similar to that. But essentially internal controls work in three aspects and what they try to control is what I showed in the previous slide. That is for a broad understanding of what is the role of control in organization.

You can look at it from the perspective of accounting controls. So that there is no fraud, there is no thing or there is nothing that can actually lead the organization to bankruptcy etc. So these are three aspects of the controls that organizations put in place for governance purpose. Now we come to the COBIT framework, the specific COBIT framework. What is prevalent today is COBIT version 5.

So you can go to COBIT site and explore further. This COBIT implementation is usually a project done by IT organization because COBIT is implemented through information systems. So they have the, so what is COBIT? So it is based on the few principles that is mentioned here. Again stakeholder needs, covering the enterprise end to end, applying a single integrated framework, enabling holistic approach and so on. So these are actually ways to understand COBIT.

So COBIT essentially looks at the entire enterprise. This is something to keep in mind. So when they say end to end, it is not looking at cyber security alone, but it is looking at the health of the organization end to end and put in place standards through information systems or IT systems to manage them, to monitor them, to control them. So controls will have specific elements as we discussed already, but this is a system for safeguarding the health of an organization end to end, health of an enterprise. So COBIT 5, when you look at it broadly, you can see it separates governance and management.

So we just discussed what is governance and what is management. So this is drawn from the COBIT standard, the introduction. So you can see what is the role of governance and what is the role of management. So governance is above management. Governance put in place the management and it directs, it evaluates and it is monitored. And so therefore, a governance framework should have constant feedback from the management systems and they should also be able to inform the management systems.

You can see that. And so the COBIT framework particularly functions based on four steps that is shown here - Plan, Build, Run, Monitor. And there are similar strategies in other standards also which you can relate to. So plan and for planning it has a separate

set of processes known as APO, build they have standard set of processes, run and monitor. So these are abstractions.

So it breaks down into us, more details as we go down. I am not getting into that. But the idea is to give you a sense of what are these frameworks. These frameworks manage health of an organization or manage risk of an organization at a higher level for the entire organization. And it is done through certain standard processes. So they actually implement this using certain processes and structures, which is depicted here.

So that is what we mean by COBIT standard. And you can appreciate that COBIT would contain cyber security or cyber assets as part of the assets to be managed. Then let me also give you an overview of COSO and COSO ERM. As I said earlier, COSO is a standard that has emerged from the accounting community. And initially it was only meant for internal controls.

And then it expanded to enterprise risk management or ERM, COSO ERM. COSO is a accounting body. It is a committee which actually developed this framework. And COSO ERM further expanded for enterprise risk management. And as I said before, they added three more elements to COSO to make it COSO ERM.

And there you can see that in original COSO, there was risk assessment. And in COSO ERM there is also risk response. So therefore, it actually became a closed loop. So you not only monitor the risk, but how you respond to risk. We will discuss this part in more detail when we discuss risk management from the cyber security perspective. What are the different options available for management to respond to cyber risk? We will see that there are five different ways.

But COSO also, your textbook also talks about it. So responding to cyber risk, when you actually do a detailed risk assessment activity, then you will find that certain assets are more vulnerable than others. So how do you actually prioritize and put in place systems to respond to cyber, potential cyber risk? Okay, so then there are actually objective setting. Objective setting here in COSO ERM would mean objectives for the entire organization, not just for risk management. What is the overall objective or management objective that the organization needs to attain and how your assets are actually protected or enabled to reach the overall objectives of the organization? So, assets are procured or assets are invested in, for reaching certain objectives. So therefore, from that perspective, are assets available or ready for supporting the organization and its objectives? So even the identification is the third item that is added to COSO to make it enterprise risk management framework.