Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

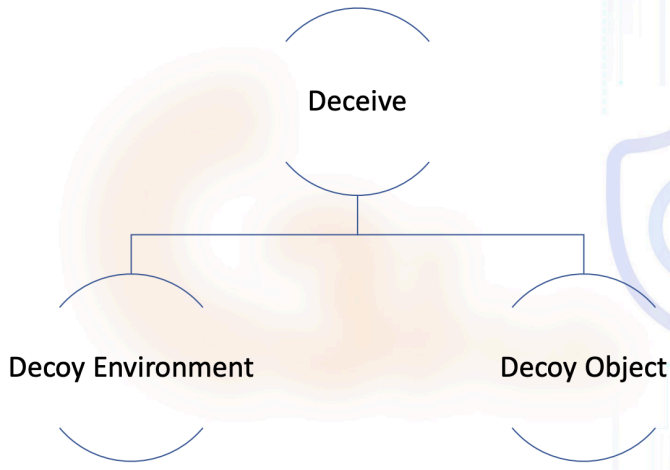
Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 18

MITRE DEF3ND Framework Conclusion & Introduction to Risk Identification and Assessment

Two parts two of the tactics of DEFEND in particular the detect which we discussed slightly in the previous Friday also and also we have discussed isolate right so how to isolate execution and how to isolate network so that in case a particular application is being exploited Then, its effect cannot move to other applications or to the platform level or in case a network component is part of the network is compromised, other parts of the network can be saved by being difficult to access from the compromised part of the network. There are two more top tactics, deceive and evict. After that, we will be done with DEFEND and we will move on to the next topic. So, deceive. So, many of you have heard of honeypots, right. So, honeypots are deception techniques, but that is not the only deception technique.

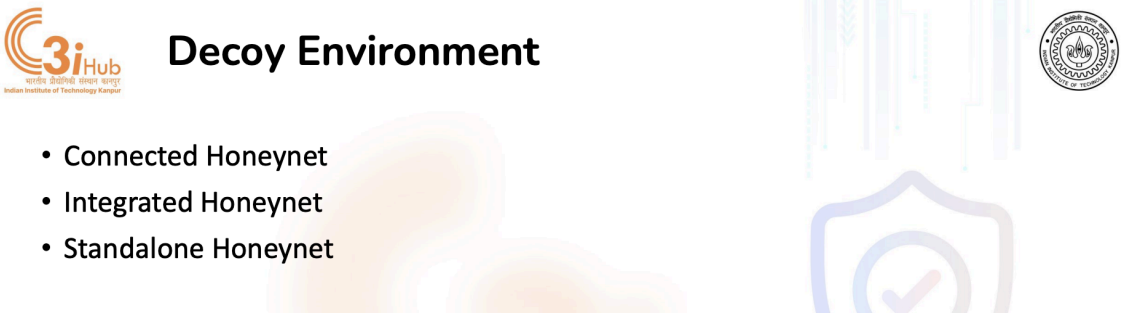


The idea is that you want to understand and observe the attacker in your network. such that you can gather threat intelligence about how the attacker behaves. And therefore, and in some cases you can actually have a you know dynamic orchestration such that once an attacker starts engaging with your system you actually redirect the attacker into a decoy system or a honeypot system. So that you can observe them and the attacker for a while.

thinks that they are actually engaging with the real system right. Of course, after a while the attacker will not be able to access things that they expected to access and depending on how elaborate you make your decoy system. they might understand it very quickly or they might understand it after you know some time and the more time they engage with your system the better intelligence you can gather. So, this whole tactic of engaging decoy environments or decoy objects. to engage an attacker into interacting with your system is what is called the deceive tactic.

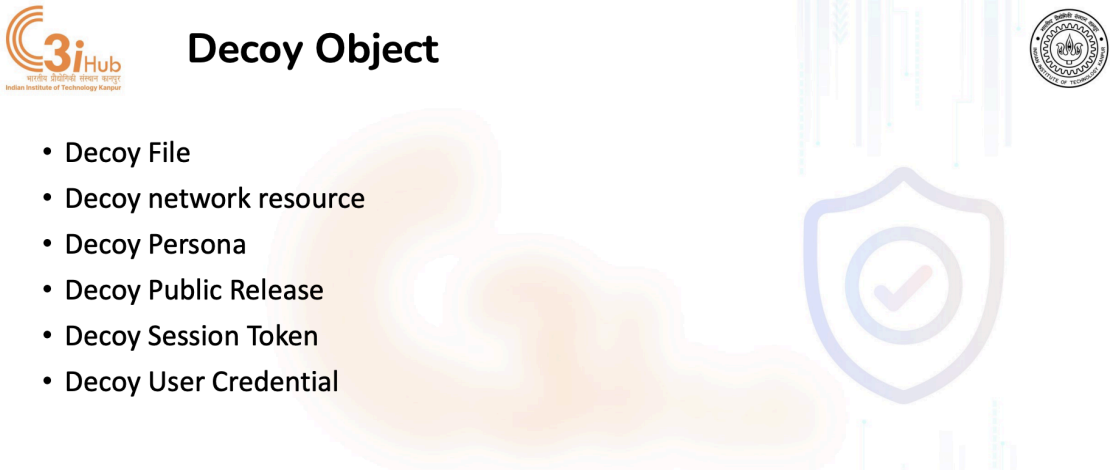
And nowadays deceit is actually not only common, it is often required for example, SEBI the security exchange board of India, they require all their regulated entities that are under SEBI's jurisdiction. to actually have high interaction honeypots. High interaction honeypots means honeypots can also be of different levels of engagement. So, there are low interaction honeypots, medium interaction honeypots or high interaction honeypots. Oftentimes low interaction honeypots are very easy to create.

You create a website with a web application with some SQL injection. some various kinds of you know weaknesses vulnerabilities in the website and then attackers will come they will try to inject SQL injection they will try to inject an XSS attack and so on, but that does not show a nature or behavior of a persistent attacker a persistent attackers job is not to just you know show to you that your website has weaknesses they actually want to get into your web server may be actually implant a web shell into web server, use that shell to you know login to your server, then actually try to see whether they can launch a privilege escalation, they try to see whether they can do lateral movement. and then eventually go and establish a command and control communication so all this stuff they will not do if they if it is just a web honeypot right so after it figures once it you know exploits the honeypot it has given itself up right so you know that it is an attacker so this that will be a what we call a low interaction honeypot. A medium interaction honeypot will engage the attacker a little more and then in the high interaction honeypot the attacker will be engaged like it is a live system. Live system there is a back end of the web system which is again connected to a network of devices with various other resources, databases and other things in there.



So, decoy environments are usually, so there are decoy environments you create such that you actually have honey pots and then you try to make it as elaborate as possible. So, you make multiple honey pots. and then connect them together with maybe software defined network or regular network and then what you get is what you get is a honeynet right. So, the more elaborate networks you have, you can also get various types of decoy DNS systems or you can get you know decoy even network environments such as that for a while. the attacker would think that they are inside a honeypot.

So, you can have standalone honeypots which are not part of a honeynet, usually those are low interaction honeypots and you can also have integrated honeypots where honeypot is integrated into an application and often you, Like for example, you can have a honeypot integrated to your web service. So, somebody tries to get into your web application, but when you see that they are trying to send you an HTTP message which has a let us say a SQL injection payload, then you know that this guy is an attacker. So, then you actually direct those messages to a decoy web service which looks exactly the same as yours. So, for a while they can engage with that object and you can observe them. So you can also use decoy files, so decoy files or decoy resources are often called honey files or honey tokens or honey credentials and so on.

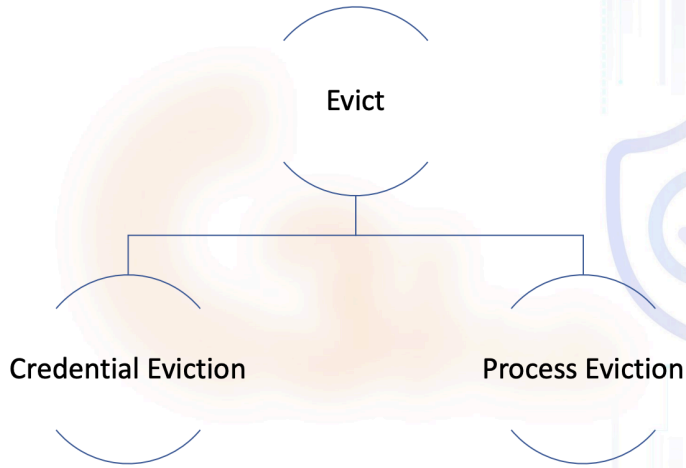


So the idea is that you know you can have a file which no regular user will ever touch. and you instrument the file such that as soon as somebody reads that file to read the file you have to basically read it from the disk and load it into memory as soon as you do that the file is instrumented to send a message to you or send an alert or something. So, that is a decoy file. So, you know that no regular user will touch that file So, anybody who is touching that file might be actually an attacker. So, that is a decoy file or a honey file or a trap file whatever you want to call it.

Similarly you can have a decoy network resource. So, you can have a particular socket that you have created and somebody is trying to communicate to that socket you know

that regular users will not. So, you know that somebody is trying to do something unusual. You can also create a decoy persona, so you can create a fake administrator and create an administrator password. So, when you start watching what passwords are being used as soon as you see that particular password is being used you know that somebody has stolen the credentials.

So, oftentimes it is useful especially to actually put such information on social media to entrap potential attackers. So, you can do decoy public release, you can create decoy session token, you can use decoy user credentials all these things to actually you know lure an attacker into doing something which would allow you to figure out what is going on who is trying to get into your system and in particular the attackers insider attackers are you know these things are good for you know check catching the insider attackers.



So, the last one in the original defend list was evict, so you have to evict from the you know if you want to if you detect that there is a there is an attacker which is you know in your system already they might have used a compromise credential or they might have gotten some way of exploiting an existing service to do a remote code execution or somehow they started a process. or injected code into a process live process you have to evict them right. So, you have to know to make sure that you terminate such activities.

Evict

Credential Eviction
- Account Locking
- Authentication Cache Validation

Process Eviction
- Process Termination

So, credential eviction is easy because you have to just ensure that from your authentication system you have removed that particular account or locked a particular account that you know has been compromised. You can also do authentication code cache validation because let us say a session cookie right. So, a session cookie recently you might have read that people were getting into Google by non-expiring session cookies, were able to connect to Google accounts. So, you have to basically invalidate the session cookies etc., session tokens etc.

, from the authentication cache. process eviction is basically you have to once you determine which process is running with some kind of a malicious code or injected code you have to terminate the process. So, what did we learn from all this right so and now if we go back here. you see that here we have another, so this is as I said that this Microsoft sorry MITRE ATT&CK or MITRE DEFEND MITRE ENGAGE this frameworks a living knowledge bases,right. So last year, we had to harden, detect, isolate, deceive, evict and evict, now they have been restored here.

So, you have to restore the system right. So, you have to for example, in case you know the attacker has stopped your access by maybe DDoS attack, the denial of service attack or by logging off users, you know you have to do restoration of the access. You may have to also restore objects like your file system or important, restore from backup disk image and so on. Similarly here you see that in the evict you have they have added this process eviction and credential eviction which we already saw, but they also added file eviction. So, this is a living database.

So, the main point to learn here is so you have to go in there and see what they are talking about and what it means. to like, for example, bootloader authentication. So, how do you do bootloader authentication? You use cryptographic signatures right, but this is not the main point. The main point of this is to understand that in order for you to actually do this cyber security profession right. So, you will be a cyber security professional you have to understand how the attacker you know how the attacker behaves with respect to compromising a system and establishing its persistent presence in the

victim system and then continuously victimize the victim by continuously interacting with its command and control server bringing in new payloads and creating more and more you know compromises, more data exfiltration, more credential exfiltration all kinds of stuff.

And then you have to understand what are the artifacts that an attacker creates in the system and then you have to understand how those artifacts may be used either for forensic investigation or for figuring out whether an attack is currently under you know ongoing. And to do that you have to also figure out what are the things that I need to monitor right. So, in order to do real time detection I have to monitor files that are coming into your system . I have to look at various kinds of identifiers. I have to monitor the network traffic, I have to monitor the host activities in the hosts and various processes, I have to monitor the user activities and behavior etcetera. But also for the sake of protection you have to also harden the system, you have to also be able to know how to isolate execution and isolate the network through various virtualization processes or containerization processes.

also through the network segmentation. Then you have to also know how to do deception, how to do eviction, how to do restoration. So this together ATT & CK, DEFEND and we defend artifact knowledge base together form a living knowledge base that would be very useful for anybody who is doing anything with cyber security especially in terms of protection of an organizational infrastructure. So, that is where we will stop with respect to the DEFEND framework. There is a lot more information here, but we will not get into that and we will move on to the next topic which is risk assessment. So, in cyber security 20 years ago people used to think. So, what is cyber security? So, when we first started using the internet back in the early 90s, we first heard of something called Morris Worm in 1988.

It was a graduate student who actually used to be a program called finger in Unix. And, what finger used to allow is that if I know your IP address or your computer's host name with the domain etc., fully qualified domain name, then I can say finger sandeep at turing dot cse dot iitk dot ac dot in. and then if Sandeep is logged in on Turing then it would show that Sandeep is logged in, what is his shell, what shell he is using, what is his home directory, this kind of information. and then if you are not logged in then it will say last login at this and this time on that so that was the finger.

So every Unix system used to run a service called finger service or we used to call in those days in Unix every service that was running on a port was called a daemon right so it was a finger daemon. So finger daemon was used by sea initially in 1980s, late 80s when ARPANET became little bit allowed in the academic institutes in the US. So, it was

a close knit community and very few people were using UNIX and TCP IP networking. So, therefore, they knew each other. So, they wanted to see whether you know some guy who they know in another university or in his own university is currently logged in because then you can also say talk at a stock Sandeep at C S Turing dot iitk dot xc dot in and you irrespective of what you were doing a talk thing will open up it used to be a single terminal right it was not like multi-terminal thing so it will mess up your VI program and all that stuff because your friend is sending a talk message so all this kind of insecurities were there so morris worm was, so this guy discovered that the finger finger Damon had a buffer overflow So this using this buffer overflow the he actually basically did a remote code execution and then this remote code execution in turn did the same to other machines on which it can do fingering right.

So this Morris worm was the 1988 first internet worm that people thought that so this networked computer. i may have a problem that somebody remotely can mess up my work. So, but then even then after Morris worm, the finger daemon was patched right and then we could still use finger daemon up until like 95, 96, 97 until they decided that this is too much you know and so most unique systems disable the finger daemon. So, you cannot do finger now like finger daemons are usually disabled. but the point is that initially people thought that was ok.

So, if this happens, all I need to do is to put up a firewall in which I will ban certain IP addresses or certain users. So, I will have protection because only a few people will do mischief and if I can somehow put out the mischief mischievous IP addresses or URLs I am done. So, initially the idea was to protect the perimeter. And then around 2001, 2002 we started getting this malicious code like what they call virus right and then people started worrying about viruses and then we started having antivirus right. Do antivirus companies start selling antivirus software because of Windows systems?

Unix did not have that many viruses. So, now Linux has a lot more worms and viruses, but in those days Unix did not have that many viruses. So, Windows became very popular. So, basically Windows 95 was a watershed moment for Microsoft and then it started becoming like this. So, perimeter security and antivirus were considered the way to do security right. So, but then what started to happen is that people started bypassing the antivirus because the antivirus was signature based.

So, you can bypass it if you can somehow bypass the signatures that are already there. Then you started also having cases where there was a virus which would sit inside your organization for machines for a long time. without having been detected or having done anything unless you actually detected through the network monitoring right. So network monitoring only you can see sometimes they are sending out some messages out to their

command and control server and so on. So at this point you said okay so I need to also do network monitoring right.

then you started seeing cases where rootkits were coming in. Rootkits are basically malicious payloads that change the code for common system calls, common system commands like ls, ps, top this kind of system calls that shows you what processes are running, what files are there, what kind of hidden files are there. So, all these things, what is how many disk partitions are there this kind of commands right including ls commands or df command or top command, ps command. So, they rewrite those codes such as the malicious code that is running that has created a process, that has created a file, all these things will not show up when you type in ls and all that stuff. So that rootkits basically made people realize that I need to also monitor what is happening in my endpoints right.

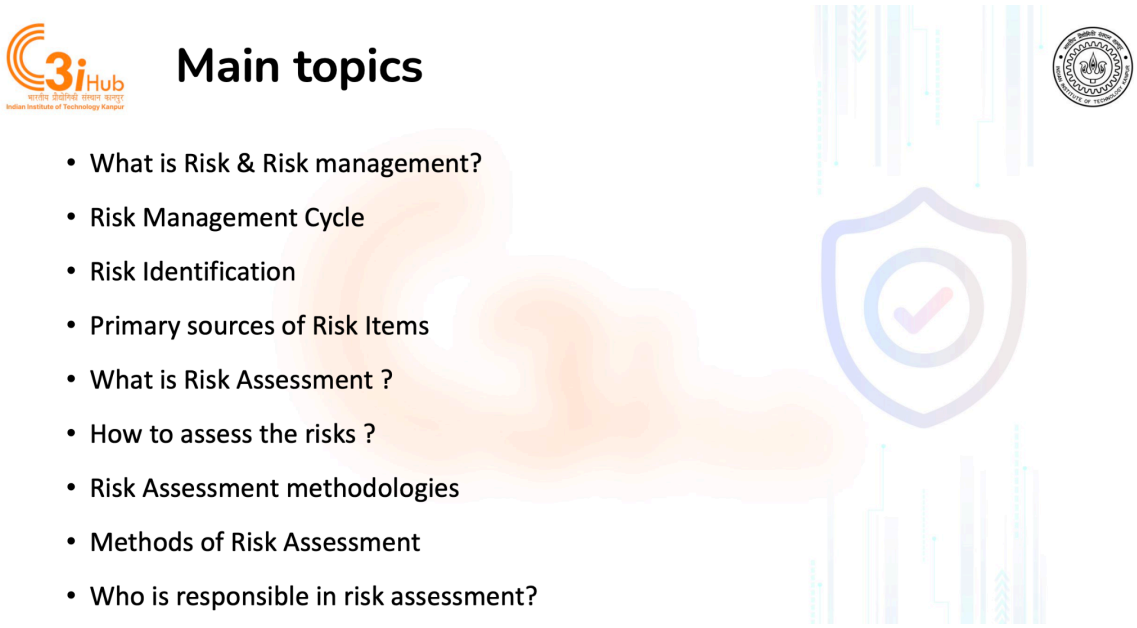
So my endpoint might create new files, my endpoint might change a binary from a previous binary to a new binary and so on. So people started understanding that I also have to do host monitoring right. So host intrusion detection. So this way we started getting more and more types of attacks and more and more types of defense as well as monitoring and detection and then how do you respond to whatever you detect you need to respond to that. And then eventually you want to check whether in case you get attacked then you need to also be able to evict restore etc.

So now the thing is that if you want to do all this in a very large organization like IIT Kanpur let us say, it is going to be very very expensive right. So you have to have you have to do segmentation of the network,you have to put agents on every machine,every host to monitor what is going on in the hosts and then, that will create a deluge of data, that will create so much data. Now unless you process that data to figure out that something wrong is going on there is no point right, see you can check your own machine but if there are usually in an organization there will be thousands of servers which are not manned at the console right so those will generate the data for monitoring data that will not be able that you will not be able to individually check whether some anomaly is going on or some activity some alert is being generated. So you have to be able to process that data so that is another expense that is another you know activity that you have to undertake. So, the expense of you know cyber security kept increasing right.

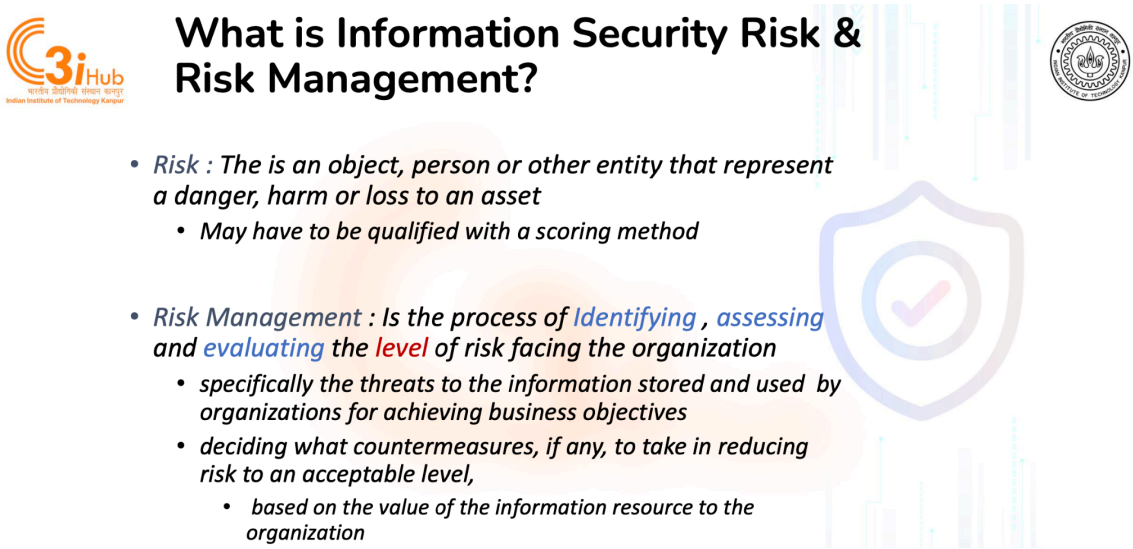
So, it becomes like in a moderately sized company it will probably a million dollar you know to actually have all that all the software for a firewalling, network monitoring, a good firewall nowadays with a which can support a you know giga 10 giga BPS bandwidth will probably cost you a crore right. So, therefore the cost is prohibitive. So, people started deciding how to actually do this within the budget that is allocated to cyber security. So, that brought the idea of risk driven cyber security. So you do not necessarily

have to put the same level of security at every part of your network or every part of your organization.

So you have to figure out which parts, which devices, which network segment is the most risky segment with respect to cyber security and then put more of your budget on that component and less budget on the component that is a lesser risky right. So that is what the risk assessment is all about, and that is why today when we actually go and do a cyber security analysis of an organization the first thing we do is a risk assessment. So, we do a full-fledged risk assessment to figure out which assets are most risky assets and which assets are less risky assets and where I should put my majority of my budget in cyber security. So, that is the whole basic basis of this part of the course which is risk identification and assessment for information security. So we want to know what is risk and what is involved in risk management. What is how the risk management process unfolds and it is basically a cyclic process you do not do this once and then done.



Because risk evolves and risk accordingly you have to always do this process. Then how do you do risk identification? What are the primary sources of risk? What are they and how do you do risk assessment? And then, then, you see what are the different existing methodologies for risk assessment and then who is responsible for risk assessment for an organization. So, what is the risk? Sorry, the word is missing here. So, the risk basically is an object or a person or entity that represents a danger or harm or loss to an asset.



and it may be qualified with a scoring method. So, risk is basically some kind of a measure of a harm that can come your way or to come in the way of an asset. so risk management is the process of identifying, assessing and evaluating the level of risk facing the organization so identification of the risk assessing and evaluating right. So the threats to the information stored and used so information security risk is about information right so We will also talk about you know risk to non-information assets right so, but in general we normally talk about like an organization. IIT Kanpur or a government department is usually the information that is at risk right, so people's data or intellectual property are the things that are mostly at risk right. So the threats to information stored and used by organizations for achieving business objectives.

So if you have data that you do not use at all for anything as far as your organization is concerned right. So my bachelor's thesis from the 1960s at IIT Kanpur is somewhere in a library in some dark corner right. So that is an example of an information that is probably have no value right. only I mean it has a value to the person who wrote that thesis right, but no value to the IIT's business as far as IIT's business is concerned right. So, will not consider that as a critical information asset, but suppose somebody has filed a patent, right in IIT and he has a formula chemical formula for a particular chemical molecule that will be useful for treating cancer right.

and that is in the computer of the user of the faculty and the student at several places that would be something that a Chinese attacker might find useful. They may want the genetic sequence of a particular disease or genetic sequence of a particular pathogen. Similarly, if you have a particular hardware design that has been patented or planning to be patented and that is an intellectual property that may be something worth stealing by a foreign agent, that might be a critical asset. Another critical asset is personally identifiable information. So, for example, all the students for some strange reason have their

AADHAR card and their PAN card and all kinds of information stored in the IIT system on servers.

Those are personally identifiable information. This course or the CPI of students, their role numbers, their names, their father name, their parents mobile phone number, all that stuff is personally identifiable information that is a very critical asset. Why is it critical? Yesterday it was not critical, but today it is critical because the DPDP acted right. The DPDP act says that in any organization that loses this kind of personally identifiable information which they collected. will be fined up to 250 crores right. So 250 crores fine if it happens of course they will not find that much to an academic institution, but if an organization is found responsible for negligence to protect that such data, the fine can go up to that level right.

So that will be a critical asset. So all kinds of informational assets are critical assets. Now what else is a critical asset in IIT Kanpur? In IIT, IIT has I believe three substations, right and 3 substations and one of them is a large 33 kilovolt substation near the health center right. That is a pretty large substation and then we have one near you, opposite here towards the market, the shop C. That is a 11 kV substation there is a 11 kV workstation near the technopark. So, all these substations have devices, programmable logic controllers which if they are attacked There could be not only blackouts on campus which may be difficult to restore very quickly. There could also be explosions, transformer explosions and so on.

So those are critical assets, but those are not information assets. Those are more assets that are equipment. So, those things actually you have to figure out what assets you have. on which there could be threats. So first of all, we already discussed that the information about personally identifiable information about students, about employees of the organization, those are critical assets and there could be threats on them by exfiltration of that data.

or ransom you know by encrypting that data you can actually stop for example, processing of registration during the registration period or grading of during the grading period you can do all kinds of attacks on that kind of data. Similarly, on the substations you can make attacks in order to create blackouts you can also there is a sewage plant near the media center. So, you can actually attack the sewage plant to spill sewage. This happened in Australia in the one of the first attacks on process control instead of an information asset was in Maroochy Shire sewage plant in Australia in 2000.

So a disgruntled engineer heads the organization you know. fired him, but did not expire his username password. So, by using his username and password he got in and spilled the

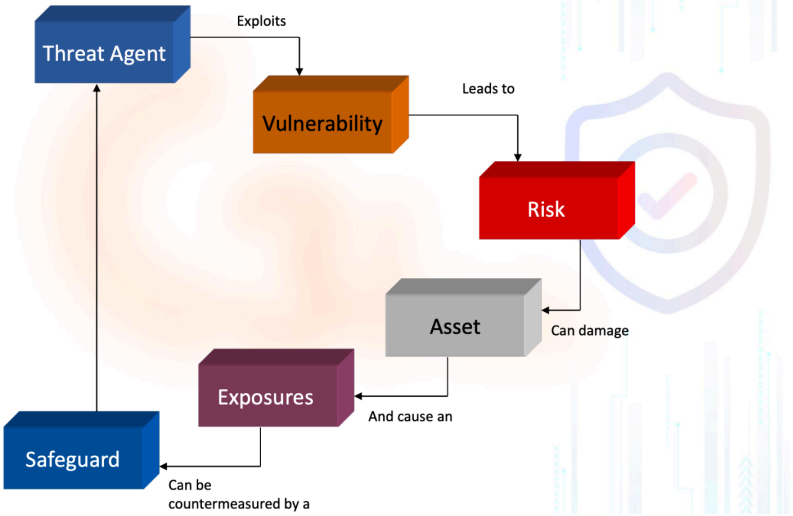
sewage so much that the entire city was filled with sewage right. So, that is one of the possible threats. So, understanding the threats to the information or other kinds of assets, digital assets, which will which will be which are used for achieving your business objectives, so it is very important to connect this to your business objective as I was saying that the thesis that are may be stored in some corner of the library from 1960s may not be important for achieving the business objectives but if you are if IIT is patenting things that kind of data is important for its business objectives and then you have to decide which countermeasures if any to take the take to reduce the risk to an acceptable level.

So risk is also never zero. So you can never get a zero risk situation. So like you are living life with risk. You are going from here to your room on a bicycle who knows somebody will hit you from the back. it can happen right so there is always risk so if you want zero risk you have to sit underneath your bed and pray that the bed does not fall on you right. So since there is always a risk there is people leaving with an acceptable risk we decide for ourselves what is the acceptable level of risk.

So, similarly an organization has to decide what is its acceptable level of risk and this acceptable level of risk. has to be quantified and has to be understood by all stakeholders. So, at the board level for example, in a company this kind of decision has to be made that this is a level of acceptable risk. For example, if you can quantify the risk in terms of money you can say I am with maybe a loss of 1 million dollar, but if the loss is above 1 million dollar it is not acceptable. So, I have to do my risk management in such a way, so that the loss is never above that level.

Now risk is such a thing that you do not have to necessarily manage yourself. You can also transfer the risk. For example, you can take cyber insurance. If an insurance company is willing to insure you for cyber incidents, then you are basically transferring the risk.

But the insurance company is not foolish. So they will come and audit you. and see that you are doing your due diligence. If they say you are not doing any due diligence, then they will not insure you. So transferring the risk is not like you treat the risk completely like a hot potato and put it into the lap of the insurance company.



Insurance companies will also want you to do the due diligence. So let us see. So what is the risk lifecycle? So threat agents, so a threat agent could be a you know threat group a insider, it could be some activists you know depending on your businesses situation for example. During the 15th August or 26th January, we got a message from the government that the Malaysian cyber army is trying to deface Indian government related websites. So, IIT Kanpur has to take special care at that time. to you know make sure that this thing does not happen right. Similarly you know you can get that during the G20 summit in September there were I do not remember the number I think 15000 attacks per second or something was happening on the G20 website right.

So, you have to understand you have to imagine what would happen not only based on you knowing what system you are running, but also your geopolitical context right, inside in your geopolitical context you have to understand who are your threat actors. So, threat actors will now look for vulnerability. So, remember they will do reconnaissance, continuous reconnaissance they will find vulnerabilities and then they will. exploit try to exploit the vulnerabilities which will lead to risk for your organizational business processes.

So risk is not to an individual risk is to the business to the business right. Eventually every organization has a business to run and this business will be impacted if an attack happens. Now if the attack is small, like defacing a website which is not an important website, maybe the risk is very small. But if it is the main website through which the organization does its business, if that website gets attacked it might have a huge financial impact. So depending on what vulnerability has been exploited on which system your risk will be different. Now the risk is usually going to impact the assets which are involved in

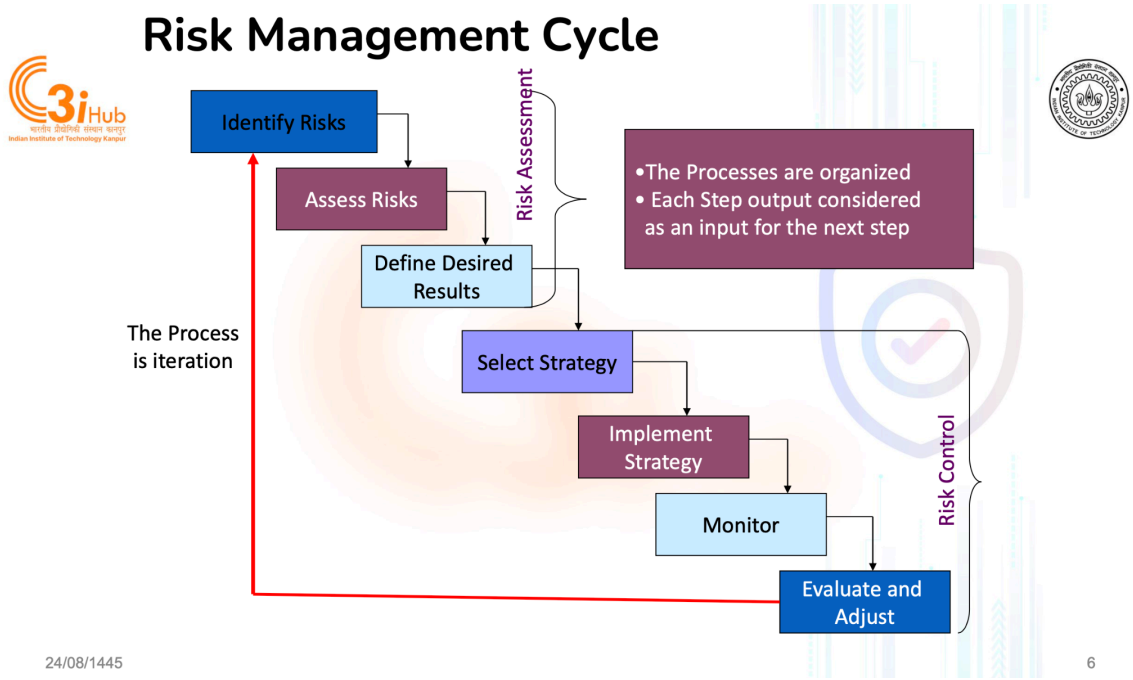
a business process.

not every asset is involved in every business process. For example, IIT Kanpur's main website is hardly involved in any business process of IIT Kanpur. But Pingla is extremely important for the business process of IIT Kanpur because we are students. IIT Kanpur is there for student activities, like courses, registration, leave, all this stuff. So if Pingla gets attacked, the impact on IIT Kanpur's business is a lot more than if the main website gets attacked. Similarly, if office automation gets attacked, It is probably not so much for students, but for faculty it might be a big problem.

So they might not be able to do a certain few things. So which asset gets exploited will decide what your exposure is in terms of business losses. And then, if the exposure is high, you determine that the exposure is high. then you decide on the countermeasure. So Pingla has to be protected really really well. Whereas the main website, the main website is not going to affect the business but there is also a reputational cost.

See if IIT Kanpur's website suddenly shows that the Malaysian cyber army has now taken over this website, which is not good for IIT Kanpur's image. So there is a reputational cost. So, I would not completely discount the exposure if IIT Kanpur's main website gets hacked. But certainly Pingla getting hacked will actually create a lot more exposure.

So now you have to decide if I have a thousand dollars to decide between the two. so I have to decide what is the exposure ratio, like is it 60 40, is it 30 40, 30 70, is it 50 50, like that and accordingly I will do the safeguarding right. I will spend money on safeguarding. So I will be doing the countermeasures, after doing the countermeasures I cannot just go to sleep right because I have to see whether now after putting the countermeasure whether the threat agents can still exploit my vulnerability. Because having a firewall does not mean that they cannot circumvent the firewall or having a antivirus does not mean that they will not create a virus that will be evading that antivirus right. So I still have to continue this cycle so this is what the risk life cycle is about and this is how a cyber security professional lives.

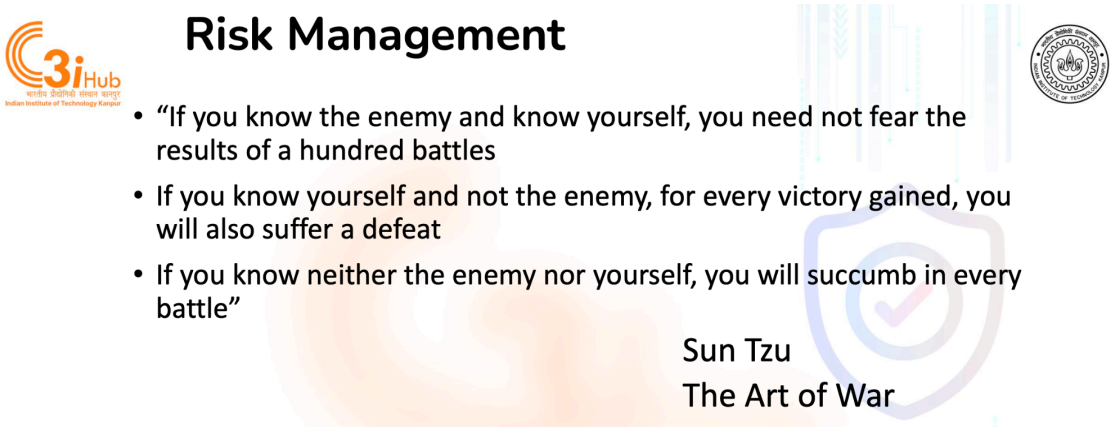


lives in fear in extreme fear of sleepless nights right. So this is basically from a risk perspective. So you identify risk. How do you identify risk? You identify threat agents. You identify vulnerabilities.

And you identify various ways threats can come from the threat agents. and then you assess risk. Not only do you need to know what is my threat, what are my threats and what are the vulnerabilities. Also I have to know what are the impacts and what is the exposure created by the attack. So, when you assess the risk. Then in the meantime you have to know what is your acceptable risk, so you have to decide what is your acceptable risk and this is not your decision as a cyber security professional this is a decision by the business guys the board level guys. Once you know that you have to select a strategy , how am I going to reduce the risk to this level to the acceptable risk level?

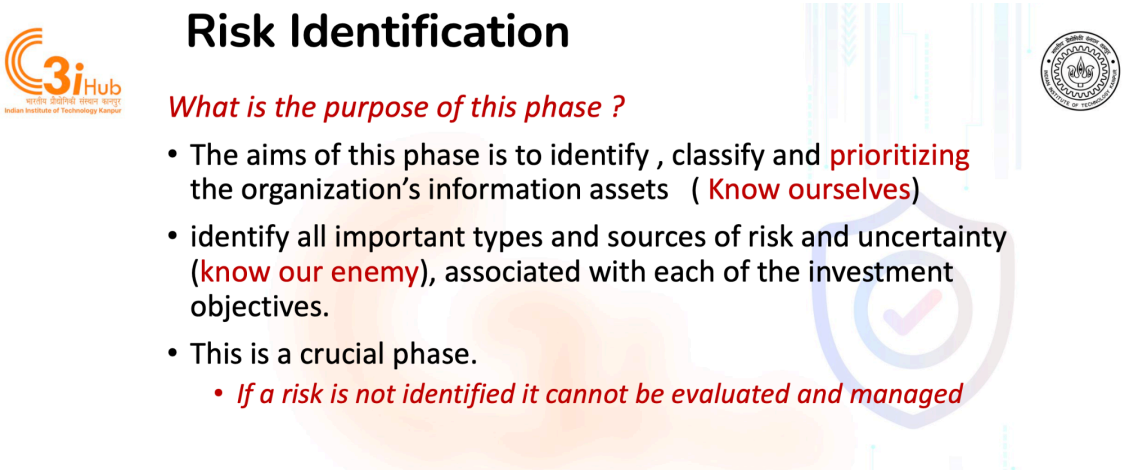
and then I have to implement those controls or those countermeasures. And then I have to monitor that the countermeasures are working and the risk is at the lower level then I have to evaluate and adjust based on what I get from the monitoring and then I have to continue again to keep identifying the risk. So, with the new countermeasures, I might have reduced the risk now for now but tomorrow there may be another risk that may come up right. So for example: if you are reading the news all the time or cybersecurity news you will see that today there is a new vulnerability in Microsoft Exchange, tomorrow there will be a new vulnerability in a moveit file copying system which is extensively used by companies, the day after tomorrow there would be some vulnerability in some firewall so there will always be new threats, new vulnerabilities, new risks right. So therefore I have to continue on this cycle forever. So this is the mantra

of cyber security actually, this is from the ancient Chinese book called the art of war by Sun Tzu, he said that if you know the enemy and know yourself you need not fear the results of hundred battles.



but if you know yourself and not the enemy for every victory gained you will also suffer a defeat and if you know neither the enemy nor yourself you will succumb in every battle. So the attack framework was about knowing your enemy. Defend was about knowing yourself, and if you know both then, you are better off. If you do not know either then you are going to have a big problem and if you know only one then you might have some wins but not always. So the idea of risk management is actually first imagine the threat actors, what the threat actors can do to your system right.

So threat modeling. Once you are doing threat modeling, once you are done with threat modeling then you have to understand what is the probability or likelihood that that particular threat will actually be realized on your system. Not every threat can be realized on your system. So at this point you have to look for vulnerabilities in your system. So, after seeing the vulnerabilities in your system you will see for every threat that you imagined whether that threat can actually happen in your system given the list of vulnerabilities that you have.



And this way you will get the likelihood that your system will be compromised. Once

you know the likelihood of your compromise, now you want to know what is the impact or exposure out of that compromise. That is if this system gets compromised, what would be the loss? If the loss is very high and your likelihood is low then, also your total possibility total expected loss will be high right. But if your exposure is very low. and likelihood is high then does not necessarily mean that your overall expected loss will be high.

So, you have to decide that and that will give you the risk figure right. So, now the formula for risk is risk is basically threat times vulnerability times impact right or exposure or consequence. So when I say threat times vulnerability I do not mean that these are quantities right, threat is not a quantity threat is a concept, vulnerabilities you know are also not a quantity. So when they write threat times vulnerability what they mean is the likelihood that a particular threat will be realized by a particular vulnerability by exploiting that vulnerability. So for example if I have a threat of data let us say the threat is data exfiltration. and you have a SQL injection in the in the web page on the web application, then you will say that this is highly likely that somebody will find the SQL injection and exfiltrate the complete database by writing a suitable SQL query right.

So, but in case there is no database, your threat is data exfiltration then that cannot happen or if there is a database but after many tests you do not find a single vulnerability that can be used to exfiltrate data from the database then you will say the likelihood is very low or close to 0 right. Now suppose the database contains only a list of items in the library right. then even if there is a data exfiltration, the consequence is very low right. Who cares, I mean it is not personally identifiable information, it is just the database of books in the library so I would not care too much right. So, in that case the likelihood may be high, but the consequence is very low right so in that case total risk is low.

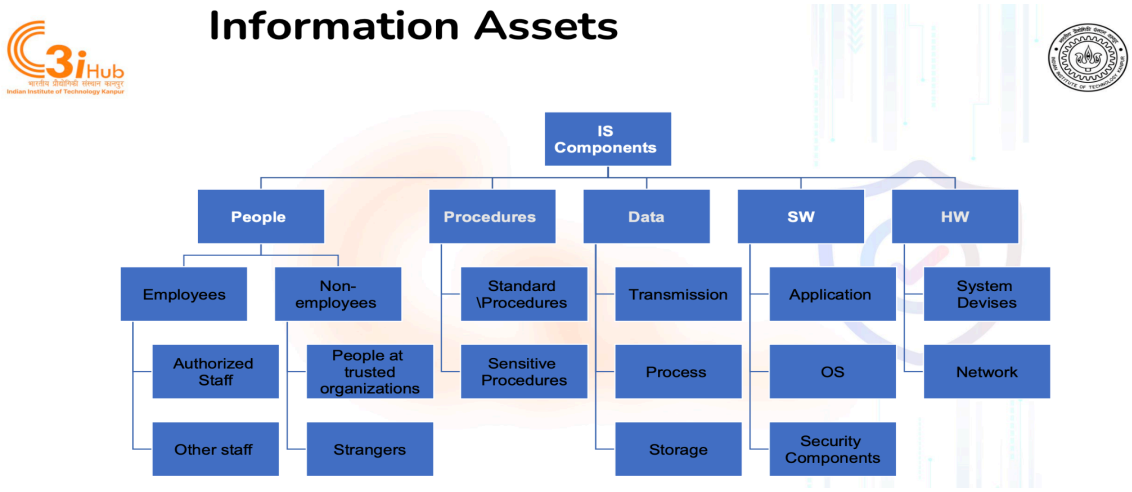
So, you have to basically figure out how to calculate the risk in terms of likelihood of a particular breach and the consequence of that breach. What would be the consequence? But we will get to that formula later right now let us look at the life cycle of the risk. So, the first thing is the identification of risk right. So to do the identification of risk first thing we have to understand is risk is to the business processes right, like whatever business processes and organization is supposed to carry out, if it is a you know let us say e-commerce business then they are supposed to run their website to take orders and then fulfill the orders through their order fulfillment system and then to deliver through their delivery system.

In that case the attacks could be either on their e-commerce website. or it could be on their inventory system or it could be in their order fulfillment system or it could be in their delivery tracking system or something right. So attacks can be in one of these. Now

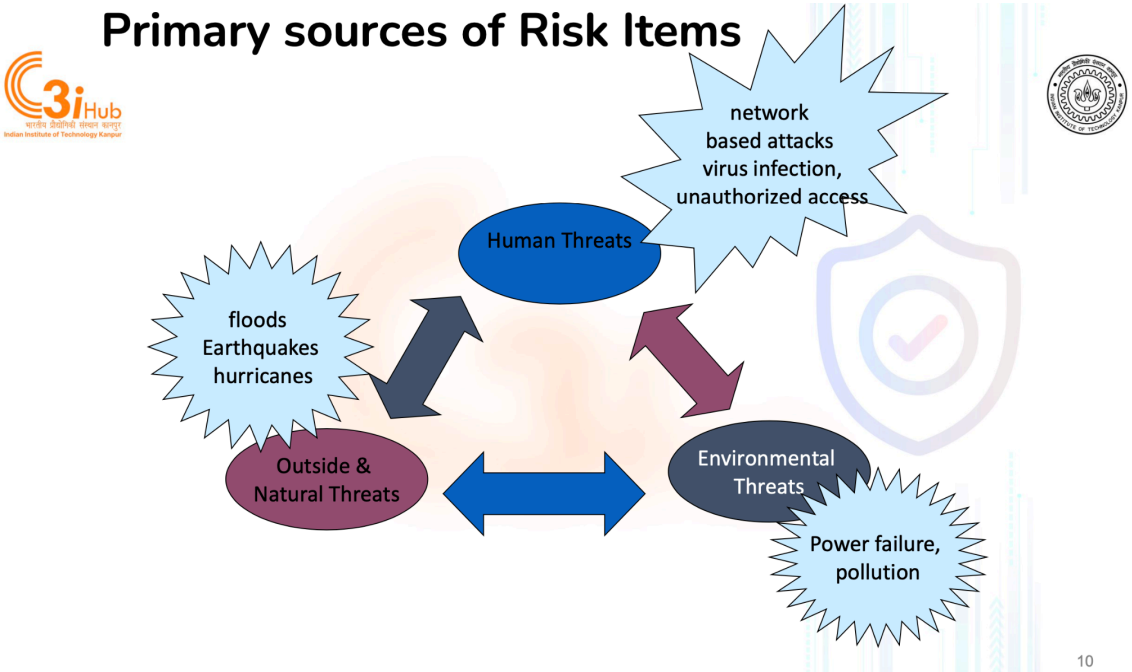
when you are thinking in terms of these you have to see what assets are involved in each of these. So in the e-commerce system for example they might be having a bunch of servers on which their databases are there, they have they are running, you know, load balancer because lot of customers are coming to these websites so they have they have number of different applications, they have number of different machines, maybe Linux Windows whatever they have maybe MySQL database or they may have Oracle database. So these are all their assets which are involved in the e-commerce front-end business process. In their inventory business process they may have a different set of servers and different sets of devices that can scan.

scan QR code or you know to keep inventory they have different devices for inventory workers to update the inventory as they dispatch things and all the stuff. So there will be a different set of software applications devices servers etc involved network devices and all that then for the for the order delivery tracking system they have a different set of applications a different set of servers so depending on the where the threat is is the threat on this business process of that business process the assets will be different the assets some of the assets may be common also maybe the same server is being used to track inventory as well as to track the So, servers may be common in both, but you have to know which assets are involved in what business process because your threats will come to the business process. So, then you will say if this threat comes on this business process, then I have to say that this asset will be impacted. So, you have to identify, classify and prioritize the organization's information assets or digital assets. So, this is about knowing ourselves and then you have to know what are the types and sources of risk and uncertainty.

So, this is what the threats are and associated with each of the investment objectives. and this is very crucial because you have to know what assets belong to which business process and you have to also know what are the possible sources of risk or what are the threats on those assets. And if you if the risk is not identified you cannot evaluate the risk and you cannot do much about managing the risk.

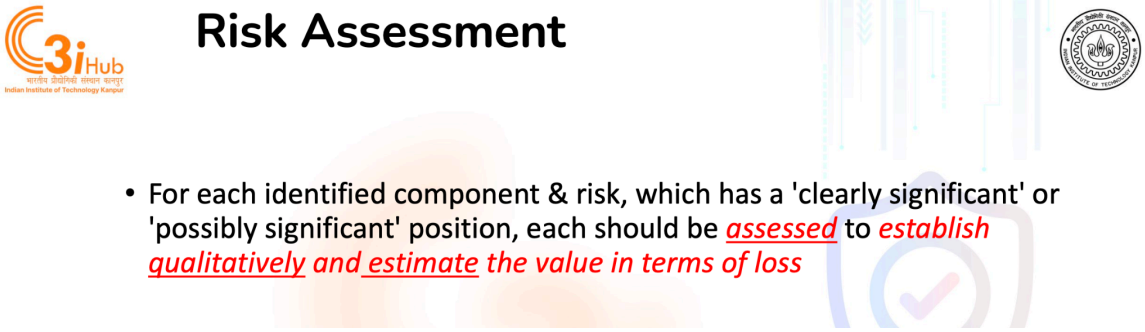


So what are the information assets? So information assets are actually you will be so you would by now you know data is an information asset, you know software is an information asset, and you know hardware is information asset. What you actually probably did not know is that procedures and people are also information assets right. So procedures means that there are certain standard and sensitive procedures like how do you do your inventory control like how do you do your you know manage certain things like for example when there is a crash, how do you restore and this kind of information these procedures and so on those would be part of your information assets.



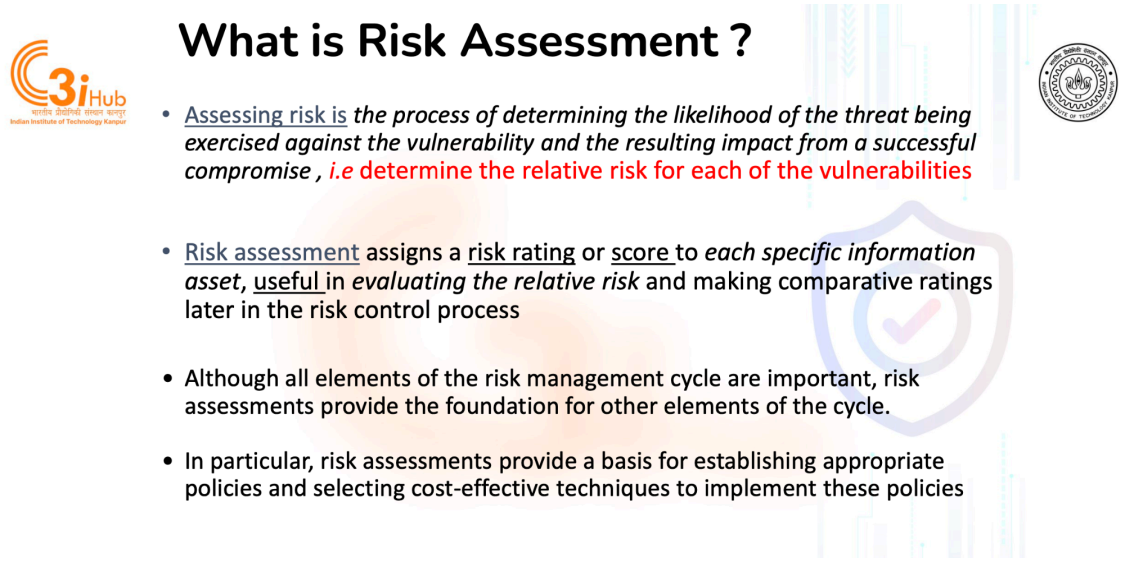
and people employees for that type of people and non-employed type of people will also be your information assets because they can be compromised. People can be compromised to social engineering and therefore there are also threats on those assets right. So, you have hardware software of course, assets operating system security

components like firewalls and you know antivirus and all the stuff applications. This is a spelling mistake. This is devices C and network and then there are transmission process storage etcetera. And then you can also have this network born as a threat. So, we are only interested in this part of the network based attacks virus infection unauthorized access etc., So, we are only interested in this type of threats, we are not interested in this type of threats, but most organizations actually consider cyber risk as part of the overall risk right so usually chief risk officer is actually is the boss of the cyber chief information security officer right because chief risk officer has to also consider all these other risks.



right and then has to always continue to compute what is the risk current risk to the organization and also they have to compute the risk to various business processes separately as well but and then overall risk and one of the risk component is cyber risk and as it gradually becoming more and more prominent source of risk is cyber right but in the context of overall risk to an organization you have to consider all the other possible risks. So for each identified component and risk which has a clearly significant or possibly significant position it should be assessed to establish either qualitatively or quantitatively in terms of loss right. So, usually it is easiest to actually talk about risk in monetary dollars or whatever rupees or whatever because that people understand, especially board level people, they understand that better right. So, they understand if you say that if you do not do this control you might in case of an attack like this you might have a known 100 crore loss right. So, they understand that better than if you just say that PII will be compromised because for them it does not matter, but if you say if you lose PII you will have a 100 crore fine from the regulator then they will understand and they will then give you the budget for that risk.

So, risk assessment so identification of risk does not give you the assessment of the risk, because now I have to assess the risk in terms of dollars or in terms of rupees or whatever right. So, assessing the risk is processing is a process of determining the likelihood of a threat being realized or exercised on a vulnerability likelihood means probability right so and then impact of that compromise right. So, if the impact is low let us say you have a desktop of the front office person who greets the visitors. So, his or her desktop may be connected to your network.



but it may be connected to an insignificant VLAN which is not connected to the rest of the servers etc. And then she has no privilege or anything even on her machine or his machine. Now that machine may be actually running Windows 7 right and as soon as you see Windows 7 you know that it will be compromised any day right. So likelihood is almost 100 percent right but impact is close to 0 right because if that device gets compromised not much data is there on that and then this is connected to a VLAN which is not connected to any of the other critical servers or even computers of the scientists or engineers of the organization right. So different networks getting from that network to another network requires you two factor authentication, a strong firewall etc.

So you can put that risk to be close to 0 even though the likelihood is almost 100 percent right. and suppose you have a server which has personally identifiable information of all students and it is very highly protected but you know that there is a vulnerability that you could not patch yet because maybe the firewall company has not dispatched a patch so for a couple of days you have to run without that patch. but you think that not a whole lot of people are using this patch using this are exploiting this vulnerability or maybe you found that this vulnerability is very hard to exploit you have to be really expert to exploit. So you can assign a very low probability that within the next 2 days before I could patch the device, I will have a chance of an attack right. However the impact will be 250 crores right because if you if it gets attacked then you are going to lose you will be fined by the regulators 250 crores then you will put the risk very high even though the likelihood was close to 0 right.

So that is how we actually calculate the likelihood and the impact. So both likelihood and impact is very important in determining the risk.