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: 07
Lecture: 21

These are the most popular groups that you see today, largely I try to not include any state actors, these are organized to cyber groups which are basically hackers for hire or their own enterprises, they make lot of money on their own, I will try to cover couple of them, so one of them is like a very very famous one which I am sure you will also read about it henceforth when you notice it now, it is called Lapsus$. So Microsoft found it first, so they gave it name called DEV-0537, they are like they have their own Telegram channels, you can also follow them on Telegram, they declare happily what they are doing and how many have got hacked, how many, how much money they have lot of things and they even invite others by saying, ok your company is not treating you well, this is the payload, please run it inside your network, we will ransomware them and we will split the profits with you. So this is the type of thing they have done and they continue to be active even today and they also try to create hype by saying we are a very simple, very simple hackers, we do not know much tech, we are not heavy tech, so which is why we are like you, we can share profits with you, I mean the different type of marketing, a different type of marketing approach Lapsus$ and of course, we can also look at couple of activities that happened in the Russian Ukraine war. The Russian Ukraine war is specifically unique because the activities that you see during the war are fought by organized cyber groups which are not known to have any affiliations with the respective governments, so the borderline fall under cyber activism, so some of the cyber groups of Russia started targeting Ukrainian and the western assets, same as some of the cyber groups of Ukraine and the west started targeting Russian interests without any provocation. What say they just started doing it on, it is like they are waging their own civilian war between them. So this was another very very important thing like lot of DDoS attacks happened continuously, independent hacker groups, anonymous have started targeting Russia and similarly Russian groups have targeted, so this type of things and there are some groups where both of them were there, they split and they fought, they shared their source code, there is a group called Conti, the group source code was dumped saying we will no longer work with Russians, so all sorts of things you know happen in the cyber space.

Now there is a huge spike in attacks because of the cyber war between them, so this is like, for example you see Quad9 is one thing which was like heavily targeting the Russian and the Poland and other the Ukrainian and the Russian countries by Russian hackers, so

there is a huge amount of activity increase from them, clear? Yeah, so far so good? Yeah, now we will little bit talk about, now we have seen the attacks, attackers and all that, now let us talk about how do we defend, how do you even know that you are under attack is the first question that I would always ask, look at these two news stories, this is about the attack that I talked about, the Bombay attack, can you guys read it? No, cannot read now I will just rezoom it, let me put it, this one, let us read this one first. This attack happened in the peak of Indochina conflict, oh sorry not this one, but yeah think about this, clear? Let us look at the other one too, it is even more interesting. Clear? So the first part of the article, the first one that I have shown you was not so clear, there is a chemical accident randomly happening, there is similar accident happened in the Neyveli Lignite Corporation also during the peak, so that probably it is connected, yeah but that being said the second article is more or less clear, is not it? What did the government of India name them? They did not name, why? This is another characteristic of the cyberspace, attribution is very very tough. Just because the server is in China, can you say that Chinese have attacked us ? Just because server is in Russia, can you say that Russians have attacked us ? It would be anyone you see, so this is the challenge that you have inbuilt in the cyberspace.

Now that being said think about it, now we care about protecting our assets, which assets we should protect most, can you protect everything? So how do you prioritize? Any thoughts? So in ISO 27000 guidelines, there is one classification called categorization of information assets. Now based on the relevance of information that is being stored within the, I am talking about the information assets only, so based on the relevance of the information that is being stored and processed within the organization, organization should take measures to categorize this information. To simply put, what you basically mean is organization has to identify what is critical to it. What do you do with the country then, how can a country, country pick what is it, but can the country defend everything? Now see the Indian Army got all our borders, what do we do in cyber, where are our borders, do we have borders? If you guys just call me on WhatsApp, mostly our traffic is going by Singapore, where is the border? We are here, I am here, how do we got the border? So we can not protect all that much is clear, right. So what do we protect is what we call as critical information infrastructure.

So we protect primarily what is known as critical information infrastructure. How is it defined? It is defined as those facilities, systems or functions whose incapacity or destruction would cause a debilitating negative impact, very strongly negative impact on national security, governance, economy and social well being of a nation. So it is a very loose definition, but still gets you some idea of what will be considered as important, clear. So under this, this is a part of the Information Technology Act, section 70A of the Information Technology Act. Now under this government of India has notified an

organization called NCIIPC, I will cover that, the organization has notified these as the critical sectors that it would want to protect first.

So we are talking about protection here which means you are not hacked yet, this is before the hack. What are the sectors? Power and energy, banking financial services, telecom, transport, government organizations and strategic and public enterprises. So the enterprises which manufacture are essential medicines, which manufacture railway wagons, ships, defence equipment, nuclear power corporation, they are all covered under this enterprise. But honestly tell me, are all equal in this list? Let us look at the relationships that they have with each other, I will zoom it a bit. Now you will understand the challenge of cyber sector.

Let us say if power goes down, what will happen next? A power grid is compromised by a cyber group, what will happen next? Can hospitals run? Can government run? What will you do if you keep all the banks everything up, no power then what? It is over? Power obviously comes first, you have power, internet is not working, what will you do next? So telecommunications, ok internet is working, neither you can pay nor you can buy nor you can move, transport is not working, what do you do? You see the internal linkages between these sectors are very very delicate. Just imagine this thing, during the COVID lockdown period I would say Zomato, Grofers, they are critical infrastructure because if they go down, half of the people will die of starvation. You have money, you have everything but then what? Think about it, we are transporting vaccines for that bit, for that stretch of the railway line it is critical to me because of that there is an accident in that railway stretch or inside a tunnel, I am gone. So that is again critical to me. So the concept of criticality is very, very fluid and very very tough.

This is the reason why governments find it very difficult to respond to the challenges, so does industries. Now as an industry you think about it, how will you define what is critical? How will you identify this is critical to me? You simply say it is profits, what about intellectual property? Access to it, employees, accidents, compliance how many things exist? How can you prioritize them and say a circle around it? So these are the complex challenges. Let us look at some of the attacks that we have endured in the last 2 years, last 2-3 years, just observe them. These are all attacks targeting India and see possible motives that the fellows would have. You guys can see it.

There are more. How many critical organizations have we covered so far? How many sectors have we covered so far? If you simply sit and make a list, you will realize all your critical sectors are being attacked one way or another and largely lot of our data is already gone out. What next? Power grid attack, correct? So we can create a taxonomy to understand the attacks also. I will elaborate this later but just for now hang on with this

one and see. It is a power grid attack, most likely a nation state.

India is to sabotage our functioning or to affect our reputation. Think about it, how would your countrymen feel or rather how would we feel? The peak of a war, one of our enemy communicates that in the right in the heart of your country I can make the lights go off. What is the message? Cyber physical, it is not just a pure cyber attack, there is physical consequences. Which means there is something that has to do with this world too, power was gone. Software hardware communication supply chain we do not know yet how they breached it.

What they have done manipulated system resource and injected unexpected items so that it crashed effectively. It is an active attack not silently ignored it is actively triggered and run. What was compromised? The integrity of the system is compromised. It was not supposed to fail. See it now, at the end of the day similar type network how many we have here? If this is susceptible, most likely they are too.

Now what is the message to us? Look at my reach, what I can do for you. So to protect this type of institution, government has created an organization called NCIIPC. It is a National Critical Information Infrastructure Protection Center. It is a long tongue twister, but if you understand the word critical information infrastructure, it is easy. It is a nodal agency established under section 70A.

So it designates and issues lists of critical sectors and issues guidelines on how those sectors must be maintained. So it sets standards. You are an oil sector, you are power sector, so you should follow these guidelines and if you have any incident or any suspicion, please report that to us. We keep monitoring the cyberspace, whenever I find something, I will tell you. When I tell you, you better do it because it is not about your business it is about the whole country now.

Clear? So these are the sectors, we have already seen this part. The challenge in India always continues to be this.There are so many agencies. Even now, we have seen, we have not talked about a very important agency called CERT-in. So far we have not talked about it now because CERT-in role immediately begins, when there is a breach.

CERT-in literally means computer emergency response team. So it is an emergency response. Emergency response is after an accident, in this example after an attack. The job is to come and immediately put bandaid, bones, skins everything and say okay, okay now you are up and alive again. Correct? Now where does the role between the NCIIPC and CERT-in come? The logically probably it means the NCIIPC job is before the protection, CERT-in is after the protection.

But is it easy to split it like this? CERT-in also, as they have listed on their website, they also provide audits based services, so companies should audit their organization. So also there is one more thing, there are different organizations that follow along NIST, ISO and other guidelines as well. So how many in today's scenario, the Indian organizations, what do they follow exactly? Are they following these audit, what are the audit guidelines if they want to, in this realm of cybersecurity? See, basically CERT-in is an agency which regulates the cybersecurity industry in India. How do they do it? By saying that I am empaneling this list of companies to give you a certificate that what you are doing is safe, something called the 'Safe to Host' certificate, correct. Now government of India, unless and until it is exceptionally critical system they do not expect you to follow any standards.

But the companies follow for their own benefit, international standards like ISO 27001. Like you said, this is something that everybody would like to follow, to give assurance to to their customers that okay, your data is safe with me, to the investors proprietary technology is safe with me, nobody can copy it. And to get a certificate of ISO 27001, it is recommended that you follow certain empanelled guides only. Because now there is an independent agency CERT-in has nothing in, nothing for itself right. It wets and says these 10 companies can give you that certificate because I know they are good, tick, tick, tick, tick done.

So only then you take certificate from them, which way most of the banks let's say I am regulator like bank, like RBI, I am asking you as a bank are you safe in cyber ? How can you answer that question ? I have given you a framework, how do I know that you followed everything? So the easy way for you to tell me, " Sir dekho, this is a, this is a certain empanelled organization, they have audited me and they gave me a certificate saying that I comply with all the regulation that you want me to follow. That is an independent proof, correct. Now let us say, I am an international bank with a national branch, Indian branch, now I will also follow European guidelines or I will definitely follow international guidelines like ISO 27001 or NIST framework of USA, NIST frameworks, ok. It is largely left to us, there is no guarantee as such, but if you are a critical infrastructure NCIIPC issues separate guidelines, you have to follow them and they are to be read with your regulator guidelines, your regulator is also issuing one, they are also issuing one. So, you have to harmoniously read both and in case you are breached, CERT-in also issues one and when there is a breach, do you really think people will stop without stealing money or destroying something, something like that would happen.

So, cyber crime also has their own list, the cyber crime police branch will come and say, "Ok, what happened, you tell us everything. " You see that way, we have like huge number of organization which deal with this. Now your regulator is also worried let us say, you

are a bank, RBI is worried "Yaar you lost the money, now how do I answer to all the depositors ?" Now you see how many people are playing an active role in this space. This is a big challenge in India, honestly if you ask me, I hope the, this clarity comes up then everything will be much better for everyone, yeah. So, this is a taxonomy which I have just given you as an example, you seen in the Seibel grid act, right.

So, this is a general taxonomy which some academicians have brilliantly made and unfortunately I am not able to remember the paper. So, this is a brilliant way to understand attacks, I can run you through couple of examples so that you can get an idea, but before you do that, just remember the key points. Who is the source of threat? What is attacker motivation, scope of the attack, domain, which part of the world? Is it the information technology or the, my machinery which is called OT ? So, regular computers in the office are called IT, my machinery in the factory is called OT. The difference is this, it is called operational technology, I should include this in the concepts only, this is information technology. I am sitting in the headquarters compiling reports, sending emails, receiving emails I become part of information technology, I am running a machine which generates outputs, measures values, packages and all that, this is OT.

So, every organization will have both of them IT or OT, OT leads to more dangerous outcomes. It is a chemical factory, blow up, nuclear power factory, leakage, we will see couple of examples. So, this gap always exists in theory, the hackers always enter from here and want to go here. So far clear? Yeah, there are like attacks on every sector, let us quickly run through couple of them. Daimler Chrysler lost their intellectual property rights for a car and obviously, one of our friendly, one of our not so friendly countries, have built a car which exactly looks like that couple of years later.

How many billions of dollars lost? I will leave it to you. This is a very funny thing. So, an employee was very upset with the management for firing him. So, he mixed drinking water with sewage by manipulating the control system with a simple radio, running around the sewage plant. So, just travelling around in a car, kept on broadcasting message open the gate, open the gate, open the gate, clear.

So, he held very old attack a similar type like that, is the ransomware I think yeah, sabotage this is pretty decent one, but 2016. Crypto mining I am sure you all know, but this time it is on SCADA machines not on the IT infrastructure which means what you can remember, most of the sensitive machinery inside factories are openly connected to internet and they are so insecurely connected that a hacker could comfortably use them to mine cryptocurrencies. Understand? This is a regular, is a regular financial group one, it is energy group Riviera Beach group Ransomware, regular one. This one, I am sure all of you will remember, Ukrainian power grid was brought down by the Russians, as a

message before the war, follow my line or I will bring you down. It is a debatable issue how effective cyber weapons are, but then there was an attack on this too.

Another similar attack 2013, now this attacker could have practically blown up, but he did not blow up, for whatever god known reasons, thank God. Stuxnet the most famous of all, how many of you know Stuxnet? Anybody else, anybody else? Ok. So, let us ask him, he has not spoken so far. What is Stuxnet, Babu? Stuxnet was allegedly a US based attack, it was done to like, the Iran was trying to develop nuclear weapons. So, to prevent that, this is a type of APT, they installed it via SCADA networks to to, they altered the centrifuge speed to over shoot its limitation, to so to break the centrifuge and delay their development in the nuclear.

Very correct, how many of you understood clearly? Anybody has any doubts? I will quickly summarize it, nevertheless. So this was a first attack which had a very tangible clear outcome. The outcome that the attacker expected was to slow down the Iranian nuclear refinement process. So, they cleverly calculated the way to do it would be by destroying the centrifuges which are used in the enrichment of uranium. Now how do you destroy the centrifuges? They cleverly crafted a malicious application which was deployed on to the centrifuges.

How they did it is a different story, I am sure you guys will go back and read about it, it is definitely worth a read. What does that malicious application do? Let us say, you are a control engineer in the plant, you are looking at the centrifuge screen the common the HCI, the human computer interface screen. It says centrifuge is spinning at 20000 rpm. Happy, very happy, you go for have a cup of coffee and watch. But what in reality was happening is this malicious application was kept on showing 20000, 20000, 20000 on the screen.

In reality what it was doing, it spins the centrifuge to 40000, suddenly slows it down to 5000. 40000 slows down to 5000. So what happens? Rapid wear and tear. So by the time the plant operators realized, all the centrifuges are destroyed beyond compare. Understand, clear? So by the time they awoke, they have to rebuild the centrifuges again, it is all gone.

This happened in 2009, do not forget that. Of course, this we do not know is it an attack or attack probably it is an environmental disaster but it also had a cyber implications. Control systems are gone. Now once the 2009 attack happened, now the Iranians also understood, oh we can also do this and they happily returned the favour by launching attack on the Saudi Arabia Oil company called Aramco. But a much simpler attack unlike the so sophisticated attack that probably US and Israel jointly did because they seem to

get, same attack triton, similar type. See after the Stuxnet, the attack infrastructure moved away from your laptop, my laptop, to your factories and my factories or your sensitive installation, to our sensitive installations.

Steel mills, hydro power plant, you name it, I mean tell me a sector that is not covered in these attacks. This is a very funny attack, the publicly visible billboards on the roads someone hacked it, saying Godzilla is attacking us. People actually panicked in US. Another similar portal attack, this is also an OT attack in 2012, correct. Now let us look at how do you secure by collecting threat intelligence.

How does country secure themselves against foreign attacks? By building a good intelligence framework. What does it mean? You collect information about your enemy's operations, inside the area of interest. Now for you the area of interest is outside your organization and also lot of things inside your organization. So let me quickly go to another slide.

Now you see this. So this is your area of operations. Your hackers must be talking about you in social media. Are yaar, their firewall is weak now, their firewall module is outdated. Would you not be interested? We have got 5 emails of their top management professionals.

Their passwords are leaked now. Why do not we try hacking them? Do not you want to know? People are talking about you? Point 1. Point 2, in deep web, you may be running one random server distributing information from your product for your testing teams. Someone has figured it out, oh, this is running here. Must be on a random IP address. No domain name, nothing, but they figure out it belongs to you.

That is an end point, correct. Same conversation could be happening in dark web. Someone is trying to buy access to your servers or must have figured out a way to secretly pick up source code keys from GitHub. All this is happening everywhere, correct. So this is also source of threat intel that you're collecting by constantly watching, what is happening about me. And also collecting huge amount of data from your own devices.

You have 3 machines where there is continuous failure of login and that happened at 2.30 in the midnight and then one success. Do not you want to know? How do you know? By collecting logs from all the devices. Then what do you do with it? Fuse it into a platform called SIEM, SIEM, Security Information and Event Management systems. They basically automatically compile all the logs, do some analytics on it and tells you what you should be caring about.

They are called SIEMs which is what I roughly captured here as SIEMs, correct. They are the ones who will tell you. So this is why you have something called as SOC, Security Operation Center. What does Security Operation Center do? They constantly evaluate feedback coming from the SIEM. Now SIEM says, oh, there are like 7 - 8 break-ins inside your network which means you are screwed really, right.

So what would you do? You elevate it to level 2, level 3, level 4 and analyst with amazing amount of experience will quickly look at and say, " Sir, I think we have a ransomware attack, rapidly spreading inside our network." Ok. This is how people today fight. They collect threat feeds from these networks, fuse it with your own data, run some analytics and try to hunt for threats inside their network. You found a threat, then what you do? These are the 3 approaches that people follow.

EDR, Deploy Endpoint Detection which basically a simple way of putting anti-virus which is connected to cloud, correct. Second is called MDR. Use this information, SOC information and the endpoint information, deploy a third party outsider to come and fix it or deploy a more advanced software inside your network to do all these jobs. It is extended detection and response. So far so good? Yeah, but broadly speaking this is how people generally study.

Because of a management background, so you should definitely know this much. Guidelines, processes and all this, it flows from top to bottom like this. You have to first frame a good policy, then you have to adhere to good standards because framing because framing a policy should not be silly. We will be cyber resilient ok great, but what is cyber resilience? We will protect our critical infrastructure, what is critical? Now when you say protect, according to what standards? According to ISO standards, applicable government standards.

Now how do you implement the standards? Guidelines, correct. Now when you come down to the guidelines, your employees have to make sense of the guidelines. Then you have SOPs, standard operating procedures. Now if you are, this paperwork is solid and you are able to explain all this to your respective hierarchies, trust me 99 percent of your work is done. This is where lot of slips between the lips and the cup.

You have good policies, no understanding of standards. Policies and standards, no guidelines so that your employees have no idea. Boss is thinking we have ISO 27001, none of the employees understand it, its value. So they keep doing what they usually do, which is very very risky. So these are the challenges that you face.

So generally speaking, my advice will be like this, ok. Broadly if you are looking at as

a big company, probably you will be worried about you being a CIP threat, you are being a critical infrastructure and you have threat. So you should look at issues like vendor security. You may be safe, but your vendor is not, then what? Your vendor has access to your network. Otherwise how would you know? He is filing bills, he is collecting data, he is delivering inventory, collecting trunk boxes, everything right.

So it is not enough that you are safe, your vendors also should be safe. And factories, not to be totally ignored, smart monitoring. Now what do you mean by smart monitoring? Anomaly detection. How is anomaly detection done? ML models. Because like we said you know, if everybody understands guidelines and standards, 99 percent of the work is done. Can you trust everybody to understand? Can you create a ML model to verify this? Yes today.

I will give you a simple example. An employee regular coming hours are 9 to 6. Log in after 9 o clock. Very easy, you know something is definitely wrong with this. And there is a log in without corresponding log in from the access card. So person did not come, but there is a log in on the server, how? So these are multiple patterns that you can generate, best by identifying anomalies.

To study all this, you do not even need to do anything special, just keep looking at what is normal by observing the data network for more than 2 months, 3 months. Then observe all benchmarks which are beyond this, it is over. Make sense? This is where extensive use of ML is going to come. And ML is going to come in analysis of malware.

Now malware writers are also using ML to obfuscate what they want to do. So to fight a malware writer who is using ML, you need ML to analyse, that is another trick that is happening. So, and of course, but that being all said, this standard principles will continue to be of great value. These are basics. So, you are denying an attacker space to operate.

You are making it tough for him to operate. That is the best you can do, know, apart from everything else. Yeah. So, I want you to leave with these thoughts. When you are working for an organization, always start with these questions. Who is my attacker? Is he going to be internal or external? You should know the answers.

Keep searching all the time. What is his skill level? Script kiddie means he does not understand much of cyber. So, he will only pick easy fruits. You can convert easy fruits into traps. You create one server, which nobody else knows, nobody else visits.

Anybody who visits it, is a hacker because no regular employee will ever visit that. Unknown guy is inside the network, na? Those are traps, you can build them. Semi skilled

guy, you can still catch him with good EDR, XDR, these type of networks. Highly skilled guy, very tough. You need to deploy a separate team.

You need to have, you need to be very paranoid about your core assets. If you are a national enterprise, this is one something that you will be worried about, correct. Now, next now you found an attacker, why is he attacking you? Espionage or maybe to just demoralize you. Let us imagine you are working on a very sensitive project which will transform your company. Someone leaks your source code, dumps it on internet. A better connect, you are releasing a super hot movie, someone dumps it on Torrents tomorrow.

Go on. This is the motive. What is the motive? You should understand the motive, very important because capabilities are easy in cyber. Motives are very tough to gauge. Now, inside the network, who is the target? Then you will understand, focused or unfocused company. Make sense? Any other questions, boys? Sir, what are the, these ethical hackers? Ethical hackers are hackers who have breached, but do not want to retain control.

They just want to alert you, which is why if you look at my old slides. The payload wala slide, is basically it also had a slide on ethical hacking. This one. This is what ethical hackers do. They identify everything, except short of exploiting the situation and then leave it there. So, instead of running a malicious payload they run calculator, just to prove the point to you.

You get the message, na? They will come and tell you, you have a problem. Obviously 99 percent, nobody agrees. Then say look at your computer, the calculator will come in 5 minutes.

Ting. You know it works now. Correct? This is the sample information. It is available on the web page. It is vulnerable. Please patch it. So, guy with a motivation not to exploit, but to alert.

These are called ethical hackers, white hats, all this. A guy with the evil mind is called a black hat. And usually generally speaking, puritanically speaking, hacker is a good word. It means a guy who is interested in understanding internal workings and one who is so curious that he want to improve it by even destroying it or playing with it.

So in our times, Cracker used to be the guy who is a negative guy. Now people do not differentiate. Ya, but when I was studying in the college. So, if you have your guy cracker when probably you are not a good guy. A hacker is a good term which means you are curious, you want to understand the intricacies of every system and then do what you do not expect the person to do. Like you have a username password, type in Tamil.

Is a programmer expecting you to type in Tamil? Let us see what happens. So, that is the curiosity of a hacker. Yes sir, with the evolving of the cyber crimes, what are the, some of the you know gaps in the cyber security policy of India. See the like we covered in the presentation, the biggest gap in the cyber security policy is there is no clarity on whose role is what. There are many agencies which are trying to do their bits, like you look at this one.

There is a massive list of agencies which are trying to operate inside the cyber space. It is really tough. There is a brilliant article by Ken. Look at this, the title of the article is what? Too many cooks. Look at the agencies, how many are there which are operating on cyber space.

And first of all we do not have a good cyber security policy at all. We have cyber security policy from 2013. It is old and outdated. So, there was a lot of news about coming up with a cyber security strategy by the current national cyber security coordinator who works in the PMO. Somehow it is not come out yet. We need to solve lot of issues, like India is only country where protection and response are two different entities.

Like we have NCIIPC and CERT-in. Usually they both are under one organization everywhere, like in UK we have national cyber coordination center NCHQ, comes under the NCHQ. We also have NCCC.

We also have CERT-in. We also have lot of other organizations. Huge proliferation in India. Everybody is trying to do something, something, something, something. There is some lack of cohesion and coordination at the national level here. But I think they will do something about it, I am sure because this is, cyber security has been a great priority area for the government, at least for the last 3-4 years, I am personally I am watching it. I am sure maybe that cyber security strategy will come up soon.

Lot of people are you know, anxiously waiting to read it. Sir what kind of, there is open source intelligence techniques that are there. So do you employ open source intelligence techniques to real world applications also because from my observations in the darknet forums that are there, for example, you have lot of data breach that is out there. You can actually go and download it, for example if you go look at Zomato, Dunzo, you can get the GPS coordinates as well of what the last login was. So how do you use this information if you get and what other methods that you employ currently, that you can protect and defend the different organization, also for consulting the different organizations that are consulting you, how do you approach them, Sir ? See the information that you access from the dark web is strictly not a information that you can rely upon because you do not

know if that is actual term which came from Zomato or not.

I am being purely clear. Second part, you have no right to user information, it is not your information, let us say if it is true too because the hacker is saying it is my information that I stole from Zomato. How do you know ? Point number 1. Point number 2, Point number 2, you have right to user information, you do not have the right to user information. So if you do not have right to user information, can you capitalize on it ? Cannot.

But there is open source intelligence relays on. See the idea, see the definition is that you have to look at the definition of the open source. Open source is anything that is public and you have right to use. So this information you cannot use for actually building but then people, see this is about the people who want to follow the law. But we are here in cyberspace, cyberspace people usually you know there are many hackers who do not want to follow the law.

So they have access to all the information. Now some hacker has dumped on the forum saying this is Zomato data. So people randomly pick 4, 5 and see yeah this is. But how can we assure that that information is actually accurate. We do not know who dropped the data.

We do not know what his motivate is. Maybe it is 50 percent accurate, 50 percent not accurate. Maybe it is a plan, we do not know all that. See that is a challenge in dark web. You have no authenticity or veracity of the data. Now you go and ask the companies, mostly they say I do not know, this is not my data. Now under those circumstances, how do you give a qualified advice to a customer that this is, this is the data that is leaked out and according to our information, this and from this data is valid.

You are under threat. So but that being said, you can always advise him, probably this could be true. Please take precautions. So you stop there. You do not cross that line. Separate questions from question from this. So for example, if there is a consulting company, comes to you and we need to identify our vulnerable spots within the organization.

So what kind of approach do you follow while, I mean working with the consulting companies. So basically this engagement is called a red teaming engagement. So in the, in the market, we call this as a red teaming engagement. So what does the red team do? Help you understand how vulnerable you are by showing you where your defenses are weak.

This is very similar to ethical hacking. So ethical hacker actually hacks. Red team comes

till the point of hacking. They do not. They just point it to you and they do it in a consultative manner. They tell you I am going to test this system, only to the top leadership of the organization.

Nobody else should know. Then there is no point now. Everybody will cover up immediately. So it is called a red teaming engagement. As a part of red teaming engagement, you do vulnerability analysis, you do penetration testing, then you come up with a report, then you also depending upon the organization and the mandate they give you, you look at, okay what type of standards that I am supposed to follow, how many am I really following, what are my gaps, then you do a gap analysis, then you help them understand how to plug those gaps, again as a consulting engagement. Correct? While this, in this process, you look at everything like the way a hacker would look at it. Like a hacker would start by identifying vulnerable usernames and passwords leaked in the dark web or just doing a quick analysis of your web pages, quick analysis of your data on Github, quick analysis of your data on lot of other places, correct. Maybe he can target your vendors, maybe you can simply call up your employees and say, okay I am CEO speaking, so I do not have access to my phone, can you please tell me your OTP ? All those things.

So, the red teaming engagement objective is to test you really, are you ready for a cyber attack ? Correct. In some cases, you also do stress testing, you DDoS it and see, but that again as said, this is a consultative exercise. You may get a red teaming engagement, you do not act unilaterally, you consult then slowly, slowly grow, clear.