Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 21

Introduction to Cyber Crisis Management

So, one of the things is that, As if you are in an organization where you are in charge of cyber security, one of the biggest problems that you face is awareness, right? People are not very aware of various threats.

They are not aware of the risks associated with the actions they do. But bigger than that awareness is another issue that is in whenever there is a cyber crisis and we will define what crisis means. Whenever there is a crisis situation with respect to cyber attack for example your entire is ransomware, it is encrypted by a ransomware gang or your entire personally identifiable database has been exfiltrated out and it is now available in the dark web or if you have a tremendous you know hundreds of gigabytes DDoS attack on most of your web applications and your business cannot sustain that level of unavailability then we say that there is a crisis right. So, these are called cyber crises. Now cyber crises need to be managed because we cannot assume and this is what the fundamental concepts behind risk framework and everything.

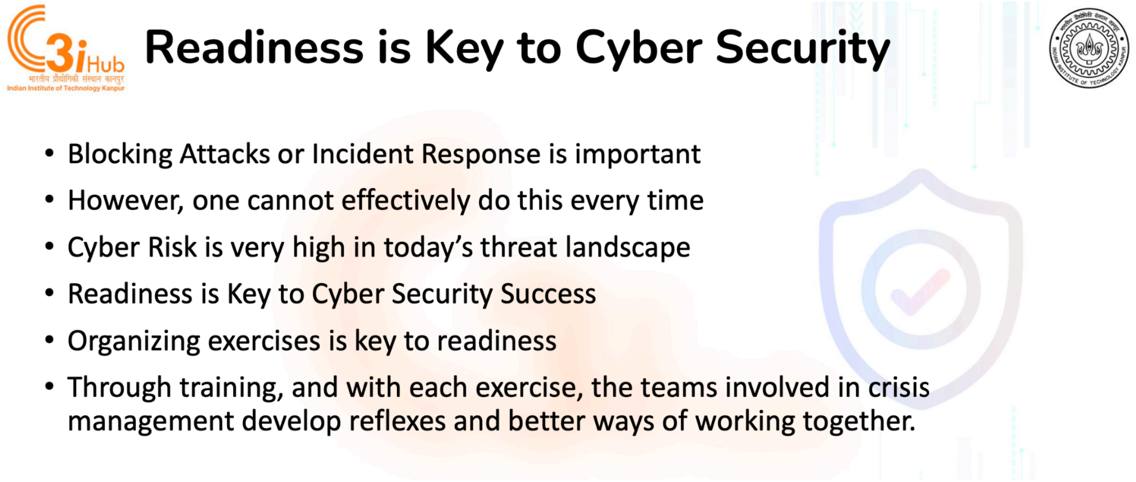
Almost every everywhere we talk about cybersecurity we talk about resilience we talk about ability to withstand a crisis such that your degradation of your services degradation of your performance is rather graceful it is not like everything collapses and you do not know what to do for a while until some you call in some emergency response team and they somehow rescue you out of the situation after several days that is not a that is not resilience that is that is a really unprepared situation. So to get resilient posture for a cyber against cyber threats. you have to be prepared and to be prepared you have to actually have plans: how do you know what we call emergency preparedness or crisis management plan also there is something called business continuity plan or business recovery plan right. So, this is where cyber meets the business right. So, because eventually a cyber crisis will affect your business and when it is the reason why cyber is important is because it affects your business otherwise why would you care right.

So, it affects your business. in many different ways one is of course your functional business functions may be inactive and therefore you will not be able to proceed with your regular business like serving customers but also if you lose data of customers then there are regulatory fines there are reputational damage which means that you will start losing customers so there is also a monetary you know penalty associated with data loss even if your business actions or processes do not stop right so business processes halting would give you a very direct monetary penalty for losing data you will get a indirect penalty in terms of if you want to calculate that in terms of economic terms so and that is why the impact like when we did the risk assessment we talked about the impact the impact comes from this monetary quantification of whatever happens whenever a cyber incident happens. So what we normally do is actually we ask every organization to have regular exercises for cyber crisis management because unless you do drills. you cannot be prepared. So, how many of you have ever been to a fire drill right?

So, whenever there is a fire drill and I do not see that in IIT actually I have never seen a fire drill in IIT, but in the US it used to happen like every quarter, right every quarter one day there will be fire alarms in the building everybody has to come down to the what they call assembly point right. So I have seen in India many buildings, not here but outside where I have seen clear signs of assembly points right but I am not sure if they actually use it. I mean the assembly points have been designed to actually carry out the fire drill where everybody has to assemble and then every floor of the of the building has a fire marshal he is just a regular employee who has been designated the fire marshal his job is to actually count that everybody who came in in the morning are available at the assembly point. In the real fire we have to know if somebody got stuck . Let us say somebody was in the bathroom and he did not get a chance to get out in time and now the fire is encircling him and he is not able to come down right. So we have to tell the fire department that there is somebody stuck on the seventh floor, probably in the bathroom or something right.

So in order to do that we have to know the exact count. So, this is how the fire drills happen and then once everybody has counted accounts, everybody goes back and this happens in the next quarter. Now, why do we do this because in case of real fire I have never seen a real fire, but I have seen this I have seen cases where real earthquake happened and earthquake time, the same fire drill came into existence the fire alarm goes off and then we had to assemble at the assembly point and fire marshals come and count us for this thing. Now unless we did this on a regular basis when real earthquake happened, we would not have known what to do right but it was a very common thing for us to actually go and go to the assembly point right nobody would miss being in the assembly point because that would create And this is why in a good well-administered building every time you go in and out you have to give your fingerprint or use your card so that everybody knows who is inside the building at any point in time right. Otherwise in case of a fire I would not know if the person who came in in the morning has gone out for lunch. I am just looking for him right now, so that kind of preparedness is required.

So you understand from the fire drill which is much easier than a cyber crisis drill, once you do this every quarter you will get a hang of it and you will not have made a mistake in case of real fire. So this is what has been emulated in the cyber crisis drills and this is required. So European agencies or regulators US many US regulators require that this be done on a regular basis for cyber crises also like fire drills. So the what you are saying here is readiness is key to cyber security by the way this I created this slides from this French national cyber security agencies document on cyber crisis management.This differs different jurisdictions define it differently but just one example is sufficient to give you an idea of what you should propose in case you go and work for organizational cyber security somewhere you should be able to tell them that this is something they should do if they are not doing it already.



Readiness is Key to Cyber Security

- Blocking Attacks or Incident Response is important
- However, one cannot effectively do this every time
- Cyber Risk is very high in today’s threat landscape
- Readiness is Key to Cyber Security Success
- Organizing exercises is key to readiness
- Through training, and with each exercise, the teams involved in crisis management develop reflexes and better ways of working together.

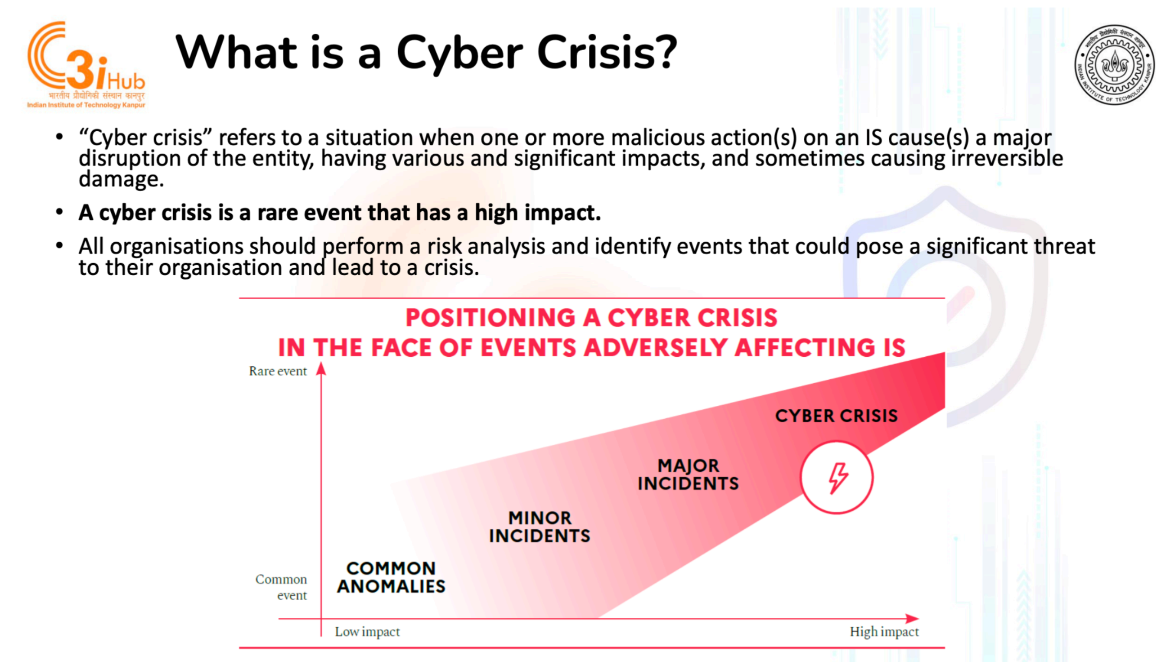
C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

So what we are saying here is that we cannot always block the attack right, so attacks are going to happen right, so we have to be ready and sometimes the attack could be rather virulent right, so it could be like you might have seen that Microsoft is now fighting the Russian hackers inside its system and they have not been able to evict it right. We talked about eviction, but they have not been able to evict it and they have admitted that source codes have been stolen right. Source code getting stolen from Microsoft rather concerning for all of us why because that source code might have vulnerability that are not known easily but they could actually be exploited if the attackers have access to the source code so we do not know what source code they got but this is a crisis right so what is to be done during this kind of a crisis or when The attacks happened in colonial pipeline right, in colonial pipeline that it is a oil and gas pipeline that you know brings oil and gas all the way from Texas to eastern seaboard entire eastern seaboard of the US. and they had a ransomware attack on their IT system not on their OT system the OT system is responsible for pumping the gas and transferring it across you know thousands of miles and all that. But because the billing was in the IT system and billing was in dependent on the on the OT system because how much gas is being transferred etc it has to be into the that IT system so since when the when the IT system got ransomware they actually shut down the entire pipeline, the OT, IT because they didn't know how to quickly check whether the OT has been affected and probably because if the billing is not working maybe they will lose money if they continue to supply oil and gas I do not know exactly what was the reason.

So, it was a crisis that was not responded to very well and in fact it affected the entire eastern seaboard oil and gas supply for 3-4 days right. something that was not exercised for. Now all kinds of crises cannot be exercised because you might not have even modeled that threat right. So threats have to be modeled etc. Like for example sometimes you will hear that hundreds of giga bps you know attacks using reflected DDoS right.

So, you actually make a lot of requests with spoof IP addresses. So, my IP address has been spoofed as the source IP address for a lot of requests let us say to a large scale data supplier and then suddenly I will get a huge number of responses. From those sources that say that can lead to a you know huge storm of data coming towards me and then I won't be I won't be able to serve my regular customers because I am overwhelmed trying to figure out what is going on. So you have to think of all kinds of different threat scenarios which can lead to a crisis. but you cannot really plan for everything but whatever you can plan for you have to do exercise and organizing these exercises can also lead to not only awareness but also debug your process and procedures for handling the crisis right so you have to know how to handle the crisis.

there should be set operating procedures right SOPs right. So those SOPs etc and also any kind of technical responses like recovery backup recovery or any kind of technical responses for quickly reconfiguring your firewall reconfiguring your network segmentation etc we have we can debug those things. and also coordination right. So coordination between different teams inside the organization can also be tested under such circumstances. Now the question is what is what qualifies as a cyber crisis right.



What is a Cyber Crisis?

- "Cyber crisis" refers to a situation when one or more malicious action(s) on an IS cause(s) a major disruption of the entity, having various and significant impacts, and sometimes causing irreversible damage.
- **A cyber crisis is a rare event that has a high impact.**
- All organisations should perform a risk analysis and identify events that could pose a significant threat to their organisation and lead to a crisis.

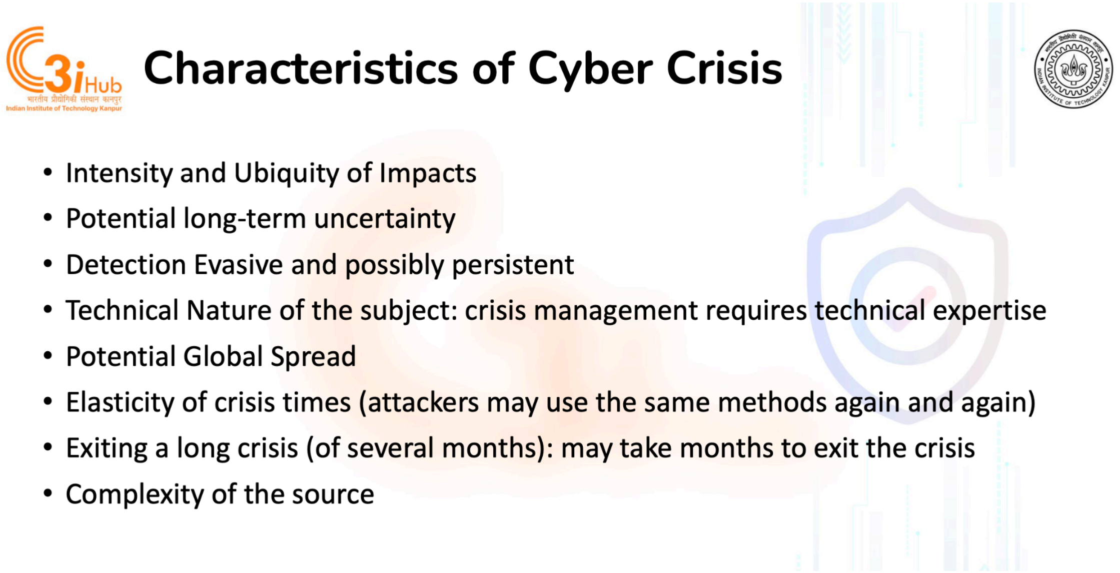
So I give you some example I gave you some example like the what happened in two colonial pipeline or what is happening in Microsoft in last few days and so on. But the cyber crisis can be so many. I do not know how many of you have heard of this book by Nassim Taleb called the black swan. Have you heard of black swans? Do you know what a black swan event is? So a black swan so Nassim Taleb made a lot of money in the 1987 stock market crash in Wall Street because he bet against what others were betting and what he bet for actually happened which was an unlikely event but it did not have zero probability. So, he talks about this in this book about, you know, events that have a non-zero probability, but a very low probability. They are very very rare, but they do happen sometimes, right. Now if you assume that the rare events are not going to happen.

Normally that is how we operate right, so we operate with the idea that events that happen in real life are the ones that are most likely right, but sometimes the black swan events happen right and then if you are usually not ready for it or you are not prepared for it. So his entire book is about why you should actually rethink the way we think like we normally think in terms of Gaussian distribution of events. So we assume that we have a Gaussian curve where the probability of events, so whenever we, the Gaussian curve is fattest in the middle right around the mean right. So we assume that those are the most likely events so we should prepare for those. We do not prepare for the tail end.

So he talks about these power laws. Power laws are actually different distributions which are called fat tail distributions where there are unlikely events that are on the tail of the curve but those events do happen because they have nonzero probability right. So here this curve is actually this curve. Here what you are seeing here is actually sort of the same story that cyber crises are the events that have very very high impact but they have less problems. So actually this curve is kind of confusing because you see the rarity of the event is on as you go up right it should have been the opposite and it should have been coming down that from the cyber crisis the from common anomalies to cyber crisis should have come you know from the northwest to southeast it should have come down, but it has been drawn like this. So you see that very low impact events are the common anomalies right, but they are most common right.

So normally we often like our intrusion detection system and everything we are often prepared for this detection of common anomalies, how to respond to them and so on. Then we have minor incidents which have a slightly higher impact. and they are a little more rare, but not as rare as major incidents. Major incidents have pretty high impact, but they have even rarer rights and then cyber crises have a very high impact, but they are also rarer right. So, you do not see that, you do not see that you know a huge attack happening to your organization on a regular basis right.

So you do not see them you may see them in like once in several years right or maybe you do not see it for once in several years maybe once in a decade right. Now the question is that are you prepared for it right because it will be extremely impactful if it happens to you right. And our mentality is that, usually we are prepared for this kind of thing right, minor incidents, common anomalies right. So unauthorized somebody this unauthorized access or somebody is trying to access unsuccessfully for several times or you know something like you know a major incident something like a limited ransomware attack on a limited set of people. or a limited set of machines getting compromised by some kind of malware etc cyber crisis would be when your entire business process is non-functional right you are unable to do your business whatever your business is if it is an educational institute your business is to serve the schedule the classes, do registration, take payments, pay salary to employees, pay scholarships and run the LMS, run the portals for you know learn the VPN, run the email system FTP system web presence web applications all this stuff is your business in case if you are Amazon, then your business is mostly on online also warehouse maintenance and all that stuff is also you know automated.



Characteristics of Cyber Crisis

- Intensity and Ubiquity of Impacts
- Potential long-term uncertainty
- Detection Evasive and possibly persistent
- Technical Nature of the subject: crisis management requires technical expertise
- Potential Global Spread
- Elasticity of crisis times (attackers may use the same methods again and again)
- Exiting a long crisis (of several months): may take months to exit the crisis
- Complexity of the source

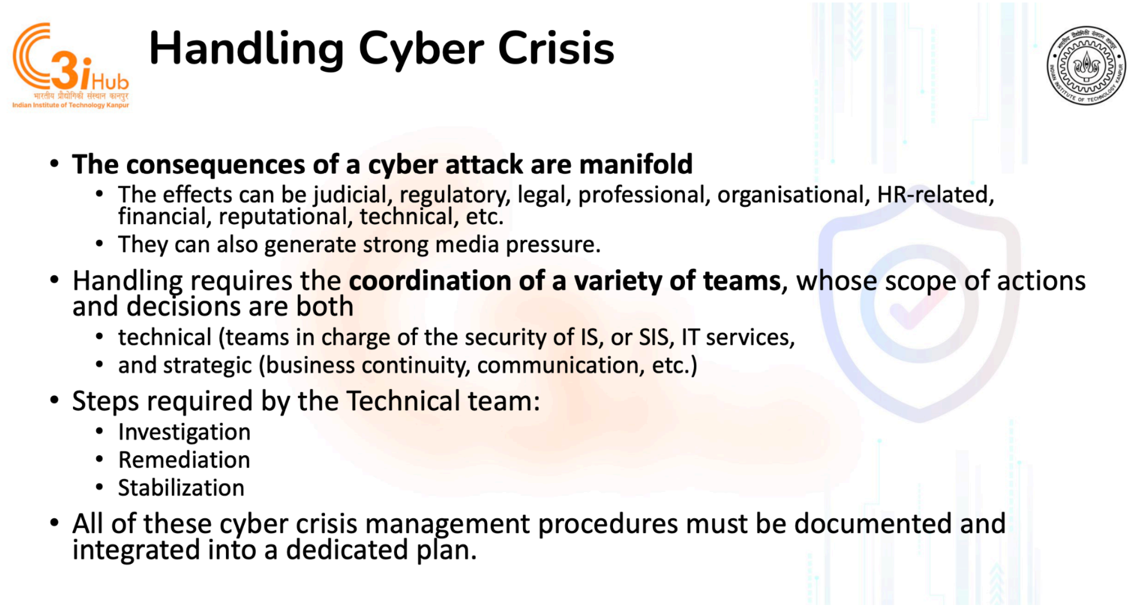
So, cyber crisis is very unlikely so we do not think about it and that is why you should read the book The black Swan. It is going to be very useful for other reasons also. So, characteristics of cyber crisis first of all its impact will be ubiquitous right. So, it would not be like you know how few people got affected in the organization. The majority of the people will be affected. right so that is one important aspect of a crisis and it is pretty intense its effect is going to be pretty intense it would not be it would not allow you to do things.

Potential long term uncertainty so you do not know when you will get out of this. Remember AIIMS 2022, I think it was October or something like AIIMS. AIIMS is the All India Institute of Medical Sciences, they got ransomware right and major for patient images and you know diagnostic images etc they all got encrypted and most probably they also got stolen we never got the full analysis of what happened because it was considered as a national security event or NIA got involved so a lot of the information is not known. But the point is that at this point this AIIMS actually went on manual procedure now for a large hospital like AIIMS going into manual procedure would lead to many days of uncertainty because obviously it will inconvenience the patients inconvenience the doctors and it will obviously slow down the process of treating patients and lot of probably patients had to be turned away and all that stuff right so that is it took many days to actually come to come back to normalcy so that is many days of potential uncertainty when this thing happened. Now then if an obviously the event that happened any kind of detection is present, usually the cyber attack that precipitated the crisis would evade the detection it will not obviously otherwise it would have been caught right and possibly persistent.

So sometimes when you start rebuilding some of the machines it gets reinfected because of persistence right so persistence could actually hamper the recovery process. the technical nature of the subject. it will be technically very sophisticated like you have to get rid of the persistence. Getting rid of persistence on a large scale is quite difficult right, one machine you can clean up but if you have thousands of machines that all have that malware sitting as a part of a startup program which you reboot the machine and it gets started up and it may be in the boot sector. So even if you reinstall everything it might still be there and all that stuff so it requires quite a bit of technical expertise right.

So that is where that is what the CERT the computer emergency response team is supposed to provide the technical expertise because not all companies have the right technical expertise. But many companies who can afford they will then bring in consultants at this point to actually help them out. a potential look of global spread right. So this could actually spread to other units, other facilities, regional offices and all the stuff plus its impact may have a global spread right. So it might actually be like the colonial pipeline had an entire eastern seaboard affected both economically and convenience wise.

Elasticity of crisis times, so the crisis times will be elastic that is it may actually keep increasing right, so crisis time you cannot really say that it is over because they can use the same methods again and again it is very difficult to rebuild create the defense at the end of this crisis you will be analyzing what happened, why the attackers were successful in making such a big attack, but at this point it may not be easy to actually mount the defenses immediately right. So, the attacker might actually come back and redo this thing, and it may take months to fully exit the crisis like in the AIIMS case and the colonial pipeline case and so on. And the complexity of the source, the source of the attack will be pretty complex, usually resourceful attackers where you know APT attackers and so on and so forth. So you get the idea about what kind of cyber incident would be considered a cyber crisis. The major thing is intensity, ubiquity , long-term uncertainty and elasticity of crisis times potential for global spread persistence. These are some of the major aspects of the cyber crisis. So now how do you handle the cyber crisis, right? So that's the point, that's what you are going to practice, right? Handling cyber crisis.



Handling Cyber Crisis

- **The consequences of a cyber attack are manifold**
  - The effects can be judicial, regulatory, legal, professional, organisational, HR-related, financial, reputational, technical, etc.
  - They can also generate strong media pressure.
- Handling requires the **coordination of a variety of teams**, whose scope of actions and decisions are both
  - technical (teams in charge of the security of IS, or SIS, IT services,
  - and strategic (business continuity, communication, etc.)
- Steps required by the Technical team:
  - Investigation
  - Remediation
  - Stabilization
- All of these cyber crisis management procedures must be documented and integrated into a dedicated plan.

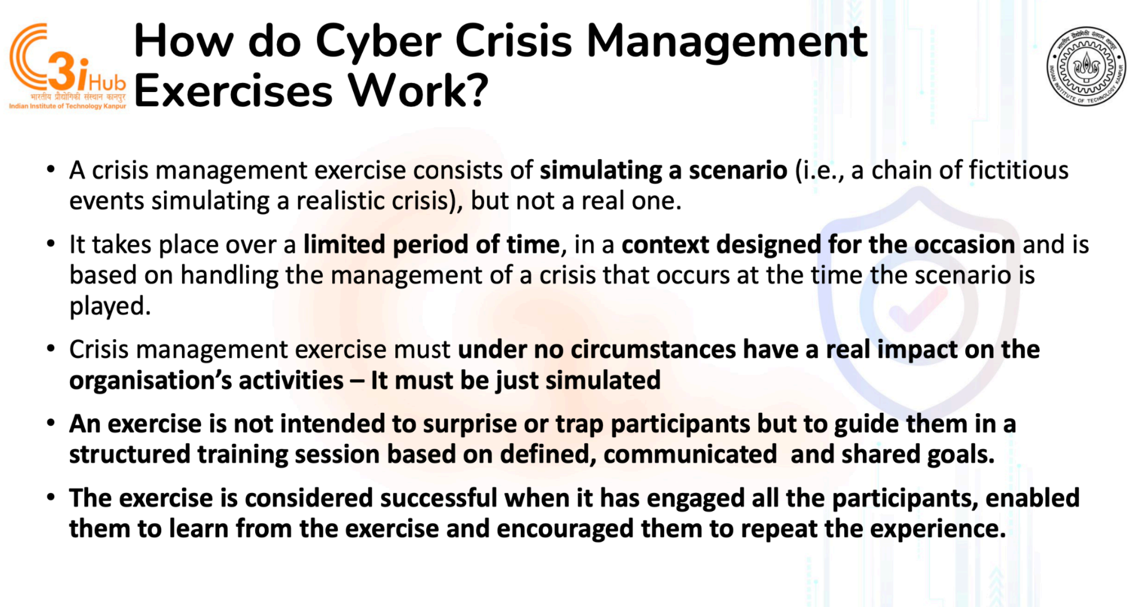
Usually incident response has to be also well planned, well documented so that there would be what we call playbooks. The playbooks will say if this happens, this is how you have to handle it. right, but those playbooks can be played out by these SOC analysts, the security operation center analyst and in the playbook it might say that ok inform the owner of this particular application, inform the top management in this case and all that stuff. The playbook should have a very detailed you know path to you know recovery from. a crisis from an incident but in case of a crisis actually the effect can be you know not only technical but also judicial, regulatory, legal, professional, organizational, HR related, financial, reputational etc and obviously media pressure can be a big problem.

So, therefore crisis handling requires coordination of a variety of teams. So, this is where it is. It goes beyond technical and it goes into the scope of you know actions and decisions like technical and strategic. So, a business continuity communication team in charge of security or SIS and IT services and so on. Now this is where. So one thing that you will learn over time as you grow is that people do not succeed just because they are technically genius, right.

Technical geniuses seldom succeed just because of their genius. Success depends on how good you are at teamwork. how good you are coordinating with others how good you are in you know taking a leadership posture when something like this happens right. So, that is how you get you know you get the attention of higher leadership and then that is how you grow in a company right. So, if you are working in a company It is seldom that you just grow, of course, technical strength gets you quite a bit far, but it may not get you to the top like you do not become Sundar Pichai just by being technical right or you know those kinds of guys.

So, and nobody told us when we were students about that. So, that is why we did not become Sundar Pichai right. So but anyway so I am telling you so you have a chance to become one big person. But in any case, you have to be able to do all that right so handling requires coordination of a variety of teams. And steps required by the technical team are investigation, remediation, and stabilization.

So, the technical team will do all this. Like they will investigate forensic investigation, they will try to remediate, fix the problems and then stabilize the system. So, that it does not keep going down and again and again right. Now these procedures that need to be done must be documented and integrated into a dedicated plan right. So this is very important for the documentation and availability of the documentation. This documentation should also be available in hard copy because all your computers may be down at the time when you have a crisis right. So you should not depend only on digital copy, you should have hard copy of this available to where it is required.



How do Cyber Crisis Management Exercises Work?

- A crisis management exercise consists of **simulating a scenario** (i.e., a chain of fictitious events simulating a realistic crisis), but not a real one.
- It takes place over a **limited period of time**, in a **context designed for the occasion** and is based on handling the management of a crisis that occurs at the time the scenario is played.
- Crisis management exercise must **under no circumstances have a real impact on the organisation's activities – It must be just simulated**
- **An exercise is not intended to surprise or trap participants but to guide them in a structured training session based on defined, communicated and shared goals.**
- **The exercise is considered successful when it has engaged all the participants, enabled them to learn from the exercise and encouraged them to repeat the experience.**

So up to this we were just talking about what happens, what is a cyber crisis and what is expected from the entire organization in case of a cyber crisis. Now we are going to talk about how to prepare for a cyber crisis assuming you have a documented plan right. I see most cases where you want to find the documented plan right. So CERT-IN, Indian CERT, the computer emergency response team has a template for cyber crisis management plan. But that entire template is wrong. The entire template is about incident response. It does not talk about crises because crises are different from regular incidents.

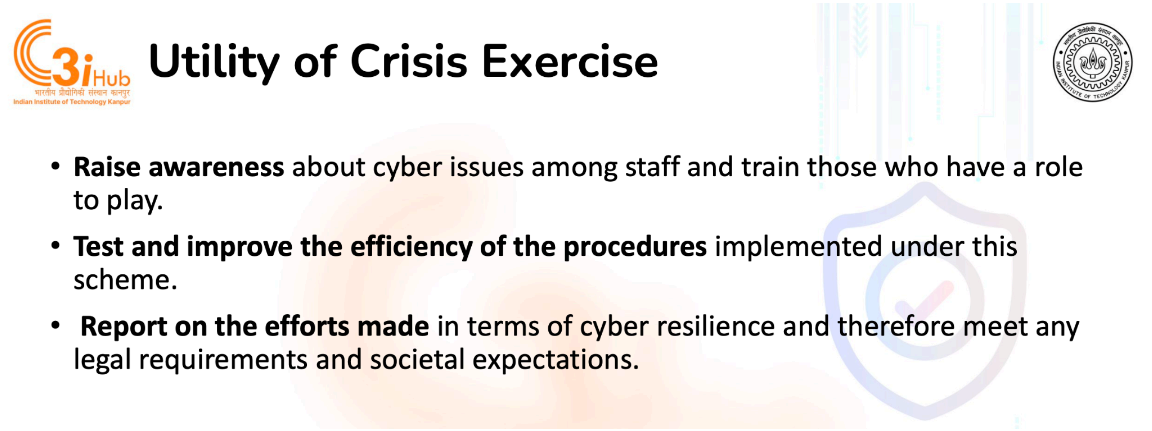
So this crisis management has to be well documented, a plan for the crisis should be well documented and then in order to do the exercise you need that documentation right. So what you will actually do is that you will simulate a scenario. So a chain of fictitious events simulating a realistic crisis but not a real one. So you will put the stakeholders together right. the CISO and the CRO and the chief financial officer and chief regulatory officer and maybe CTO etc.

, put them together and then assume that we have a ransomware attack. and assume that this they will actually create a scenario like they will say ok. So, assume that our New York regional office first noticed in the morning that there are machines which are showing ransom notes right. So, now what we should be doing at this point they will, when the discussion starts then there would be discussion there would be discussion coordinators, the coordinator will say now we just came to know that the same thing is being seen in the Washington office right. So, the crisis will be escalated as the discussion goes and then, the coordinators will notice what the CISO is wanting to do and what the risk officer is wanting to do and so on and then they will reference back to their document and say that what you are saying is not according to the plan right.

So that way they will actually help the CISO and all to get used to actually executing the documented plan rather than thinking on top of their head right so that is the idea. So it takes place over a limited period of time in a context designed for location and based on handling the management of a crisis that occurs at the time the scenario is being played. So a crisis management exercise should not have a real impact on the organization activity, it is just simulated right. Now sometimes you may have to simulate it in a rather intense way. We will talk about that you know but in this case unless you require it you do not do it too intensely. So it is not intended to surprise or trap participants right.

So you are not going to actually attack you know like one day some or you know the CISO comes to office and the coordinator of the cyber crisis gaming coordinator just really encrypts his machine that is not supposed to happen right. I mean you do not really encrypt anybody's machine or make something operational or So you want them to think you know that you know what happens when such a scenario occurs. So it is supposed to guide them in a structured training session based on well defined and communicated and shared goals. And the exercise will be considered successful when it is engaged. It has engaged all participants, enabling them to learn from the exercise and encouraging them to repeat the experience right. So everybody has to learn something from this that they did not know last time.

So in the case of fire drills for example, the first time I had a fire drill I found it a very interesting experience. First of all, I did not know where the assembly point was. I did not know that there was something called a fire marshal. I did not know that you know we are supposed to be counted and like ships and all that, But after that it becomes a kind of learning that becomes less right or almost none right. You learn more about other people during the fire drill the way they express themselves you know than about the fire drill the behavior we are supposed to do it during fire etc., But in this case it will take some time like many, many drills before you actually get you know to a point where you are learning becomes diminishing right but also in this case you can simulate different crisis scenarios at every time so that gives you a better opportunity to learn more scenarios.



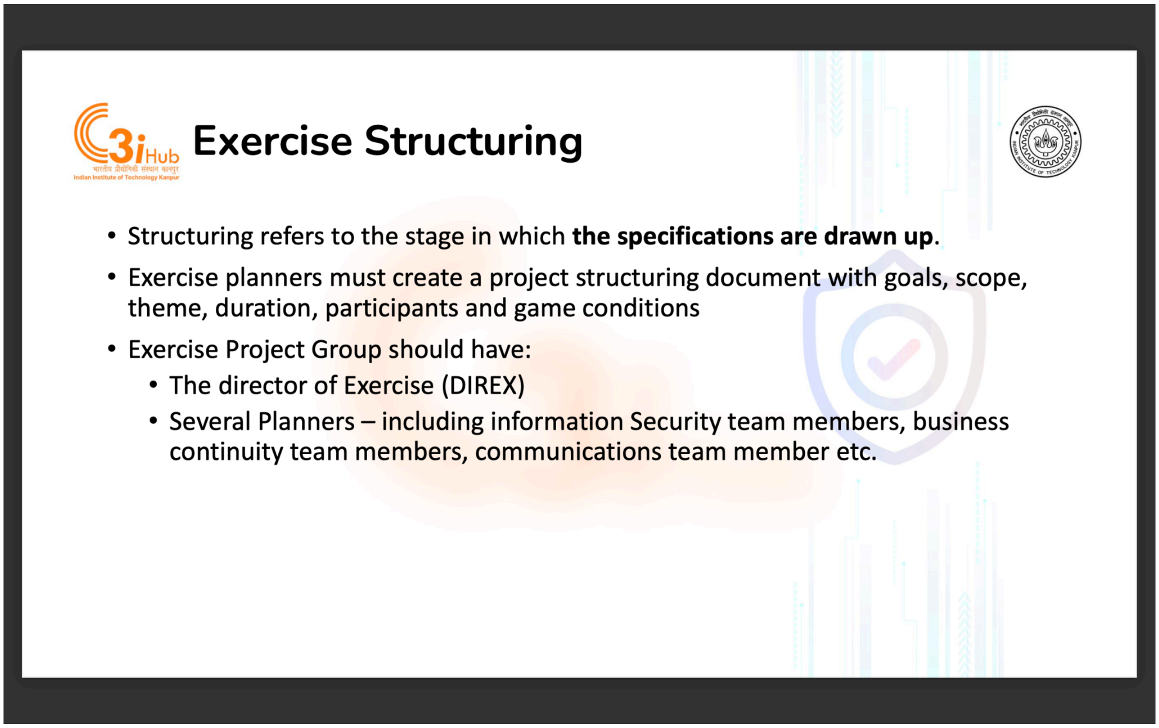
Utility of Crisis Exercise

- **Raise awareness** about cyber issues among staff and train those who have a role to play.
- **Test and improve the efficiency of the procedures** implemented under this scheme.
- **Report on the efforts made** in terms of cyber resilience and therefore meet any legal requirements and societal expectations.

So the utility of the crisis exercise is to raise awareness about cyber issues among staff and train those who have a role to play right. Not every staff has to do something during a crisis, but there are important employees who have to do something. So they have to learn what role they are supposed to play. Test and improve the efficiency of the procedures.

implemented under this scheme. So this is where you debug the documentation that you have already created for crisis management and report on the efforts made in terms of cyber resilience and therefore meet any legal requirements and societal expectations. So regulators may say that you have to exercise a cyber crisis management plan every quarter or every 6 months. So, in that case by doing this you are also meeting the regulatory requirement and maybe also the expectation right. So, you know that India is number 10 in the world ranking of cyber preparedness right. Now that I have worked with most Indian agencies I cannot understand how they can be number 10.

but they are number 10 which means that this is societal expectation so for some reason the expectation is that the Indian organizations critical infrastructure organizations are very well prepared for a cyber crisis right that's why the number 10 right but reality I do not know but on paper we are number 10.



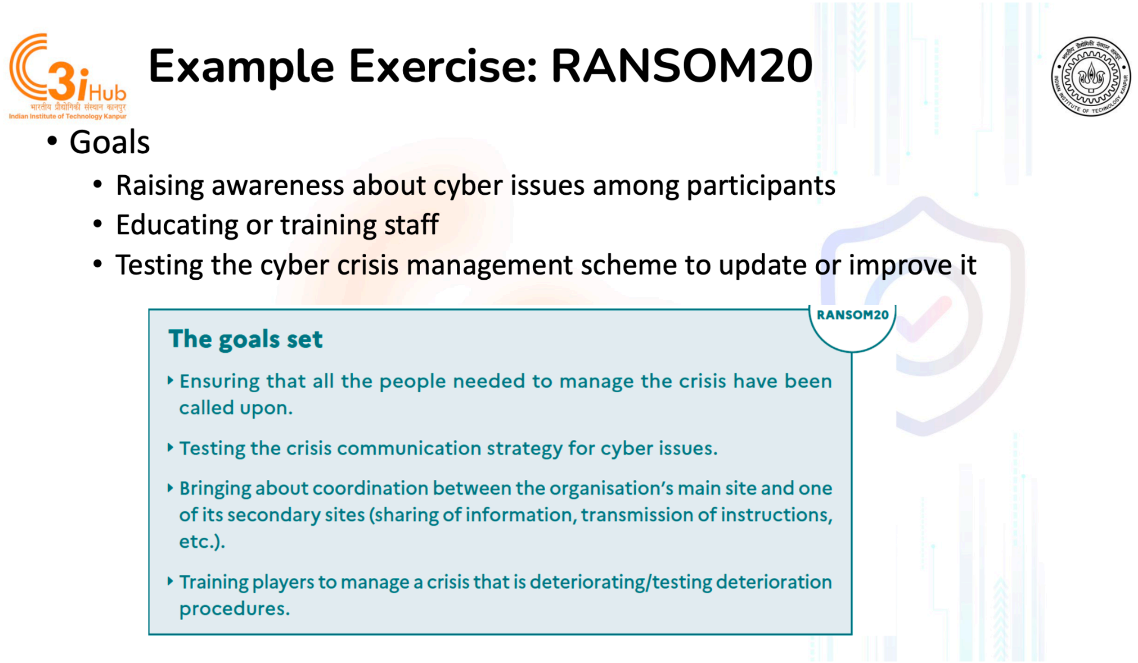
Exercise Structuring

- Structuring refers to the stage in which **the specifications are drawn up**.
- Exercise planners must create a project structuring document with goals, scope, theme, duration, participants and game conditions
- Exercise Project Group should have:
  - The director of Exercise (DIREX)
  - Several Planners – including information Security team members, business continuity team members, communications team member etc.

So now how do you structure the exercise so structuring refers to the stage where the specifications are drawn up so this is not something you just like decide tomorrow that let us do a cyber drill and do it right it is not like that you have to have plans so exercise planners must create must create a project structuring document with goals, scope, theme, duration, participants and game conditions. So these are the things that you have to document before you start. Interestingly, so last year the students who took this class last year, among them this one group actually formed a company, right, startup company that you they are actually a company of deception company they do honey pots right, but they got a project with a an academic institute called BITS RACHI I think BITS MESRA and they were asked to actually help them improve their cyber posture after the AIIMS incident actually right. and this company actually did a cyber crisis exercise based on what they learned here, right in BITS MESRA and apparently it went pretty well.

But, you can actually design your own cyber crisis management drill exercise if you want. An exercise project, so exercise has to be actually created as a project right. So the director of exercise and several planners and the planners should have obviously security team members, business continuity team members, so usually large companies will have a business continuity team and then communications team members. Now this is not network communication, this is communication in the sense of communicating incidents public relations right.

How do you handle presses when you are under attack right? So when AIIMS was under attack, the organizations the AIIMS did not much by way of communicating to the press they did communicate to the regulators and the agencies like certain they communicated to NCIIPC they also communicated to I4C who communicated to us. So, our engineers also went there and started looking into it. but then NIA came in because it was a national security incident and then obviously we were no longer doing anything. But the point is that if you are a large company you probably want to also have a press release etc about what is going on where because your stock, your shareholders and other customers etcetera may be concerned about wanting to know what is going on there. So here is an example exercise called RANSOM20 and the goal of this exercise is to raise awareness about cyber issues among participants, educating and training staff and testing the management's crisis management scheme to update it or improve it, right?



Example Exercise: RANSOM20

- Goals
  - Raising awareness about cyber issues among participants
  - Educating or training staff
  - Testing the cyber crisis management scheme to update or improve it

RANSOM20

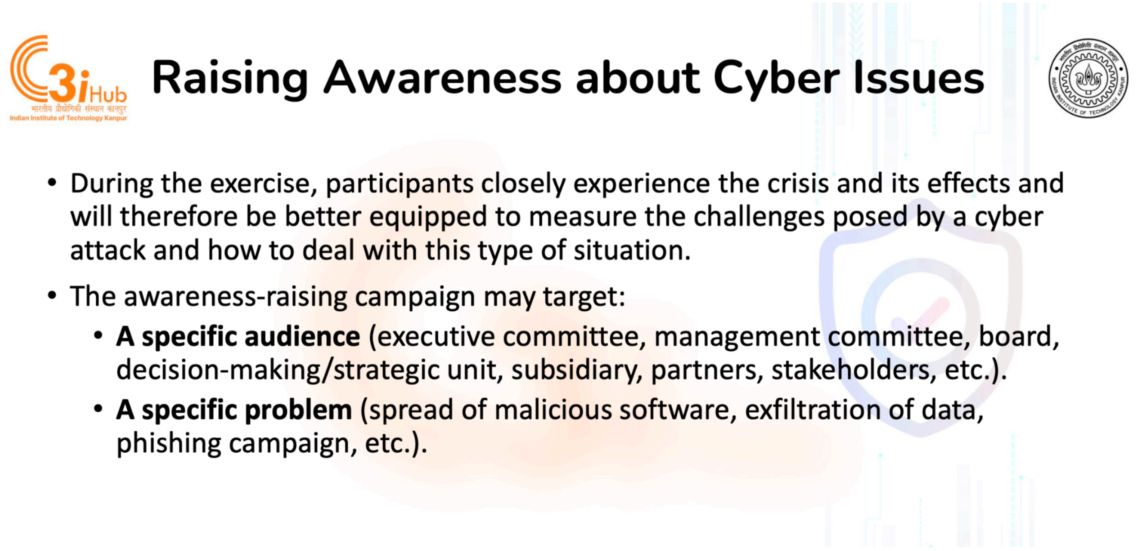
The goals set

- Ensuring that all the people needed to manage the crisis have been called upon.
- Testing the crisis communication strategy for cyber issues.
- Bringing about coordination between the organisation's main site and one of its secondary sites (sharing of information, transmission of instructions, etc.).
- Training players to manage a crisis that is deteriorating/testing deterioration procedures.

So that is what let us say you want to do. So goals are ensuring that all people needed to manage the crisis have been called upon. So anybody who is supposed to be you know involved in crisis management including CISO, chief risk officer, maybe the CTO, maybe also chief operating officer. Maybe others you know business continuity plans, you know the head of the business continuity department etc they have to be involved. So, testing the crisis communication strategy for cyber issues. So, communication has many facets, one of course is communicating to the outside world to the press etc communicating to the regulators.

So, CERT-IN for example in India the rule is that any attack you have to inform the CERT-IN by within 6 hours right that is a rule. So, you have to have a team that does that, they collect enough information for CERT-IN and send it to you within 6 hours. So, also you may have to also inform the stakeholders who you know like your shareholders or your customers etc those who got affected. and then bringing about coordination between organizations main site and one of its secondary sites like sharing information, transmission of instruction, etc. So, ideally you would also involve if your company has many sites you ideally an exercise should involve multiple sites: the main site and the other sites.

and training players to manage a crisis that is deteriorating or testing deterioration procedures. So, escalation of the crisis has to be also tested. It should not be just you know there is just a crisis happening, it should gradually the game should be done in such a way so that it is gradually getting worse. So, during the exercise participants will experience a crisis and its effects. and therefore be better equipped to measure the challenge posed by the cyber attack and how to deal with this kind of situation correctly. So in the case of RANSOM20 for example , the game coordinators will tell the participants that we have this situation where we have a set of machines in the morning. Workers came and they found that there was a ransom note and they were unable to log in right.

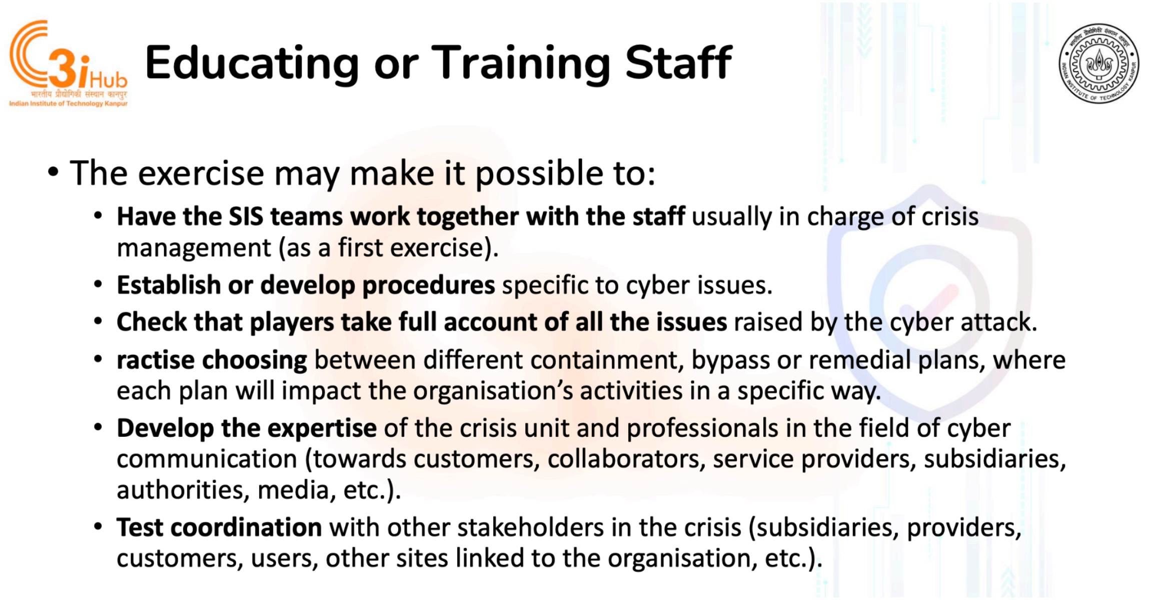


Raising Awareness about Cyber Issues

- During the exercise, participants closely experience the crisis and its effects and will therefore be better equipped to measure the challenges posed by a cyber attack and how to deal with this type of situation.
- The awareness-raising campaign may target:
  - **A specific audience** (executive committee, management committee, board, decision-making/strategic unit, subsidiary, partners, stakeholders, etc.).
  - **A specific problem** (spread of malicious software, exfiltration of data, phishing campaign, etc.).

Now at this point the game starts but coordinators know what to do right. So the discussion points could be that first of all like how you know. get the technical team to actually look into the situation and see what ransomware it is, whether there are known decryptors for this right in case there is no known decryptor is there a ransom note right and with the question then the finance and maybe CEOs will discuss like what is the what should they do should they pay the ransom or should they actually do they have backups to rebuild the system so that they do not have to pay the ransom. Then the question is what is the different data that might have been stolen along with the encryption? Is this data important and if it is then you know should we involve our brand. you know the company that looks at your brand reputation on the dark web should we engage them to see whether our data is already being sold on the dark web and so on. While this kind of discussion is going on then the coordinators will come and say okay so now we have bigger crisis we have our other site also has you know that many computers have been also having seen the same thing right.

which means that not only has it started but it has also crossed the boundaries of these network segments that separates the two sides which means that the crisis is even worse right now. So you have to actually create that dramatic effect and now the question is that depending on who is your target for this particular exercise you can do separate exercise for top level management separate exercise for regular users regular employees and so on so depending on who is your audience like is it the executive committee, the management committee, the board, the decision making or strategic units or subsidiaries, partners, business like vendors, etc, stakeholders, etc. So depending on the audience you will also have to make the story and because not everybody can take part like for example a vendor or partner may not really take part in decision making right. So in that case the game should be slightly different. And the problem has to be specific, spread of malicious software, exfiltration of data, phishing campaigns etc.



Educating or Training Staff

- The exercise may make it possible to:
  - **Have the SIS teams work together with the staff** usually in charge of crisis management (as a first exercise).
  - **Establish or develop procedures** specific to cyber issues.
  - **Check that players take full account of all the issues** raised by the cyber attack.
  - **ractise choosing** between different containment, bypass or remedial plans, where each plan will impact the organisation’s activities in a specific way.
  - **Develop the expertise** of the crisis unit and professionals in the field of cyber communication (towards customers, collaborators, service providers, subsidiaries, authorities, media, etc.).
  - **Test coordination** with other stakeholders in the crisis (subsidiaries, providers, customers, users, other sites linked to the organisation, etc.).

So you may have to do various kinds of different games. So now obviously by doing this kind of exercise you are going to educate or train your staff for example how to work together across teams right. So the SIS team is a security team. They are usually very technical and they are not very good at communication and so on but now you will have to work with the crisis management team. And this is good because later on during an actual crisis they have to be able to work with the crisis management team right. Obviously you can help this exercise will help you develop procedures specific to cyber issues. Check that players take full account of all the issues raised by the cyber attack so you understand the implications all around implication.

You can practice choosing between different containment, bypass or remedial plans where each plan will impact the organization activities in a specific way. So you may decide in different ways. You may say okay let us disconnect all the machines that have been affected so far and let us hope the others have not been infected and the symptoms are not showing up yet or you can do some. remedial plans or you can try to bypass the issue by you know disconnecting and so on. So, but each action you do will have a different impact on the organization, so the staff has to understand and this is what will be the actual impact of doing any of these will depend on the specific organization, specific network structure and configuration and so on.

And then you can develop the expertise of the crisis unit and professionals in the field of cyber communication, such as customers, collaborators, service providers, subsidiaries, authorities, media, etc. So this is about the communication part. and test the coordination with other stakeholders in the crisis like subsidiaries, providers, customers, users, other sites linked to the organization and so on. So these are some of the advantages of doing this kind of an exercise right.