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: 06
Lecture: 18

Good morning everyone. So moving ahead with the last group presentation that was basically on internet insecurity. So today our group number four, comprising of myself, Colonel Jagvir, Prasad Deshmukh and Sanjay Prasanna, we are going to present the case study that is, Protecting the Cheddar. So the case study is all about a company, Newhouse Cheese Company. It all started way back in 1811 when Cole Newhouse, he immigrated from the Wales and established the cheese making company. It got very popular, yeah in between they faced a great depression, economic depression but they innovated their business, they tied up with the supermarkets and they had a tagline-" From Wales with love.

" Later on in early 2000, the fifth generation, Chadwick Newhouse, he took over and the company invested lot of, lot of amount in the digitalization of the precision control monitors and devices. So basically, there are six characters in this case study. There is CEO, Chadwick Robert Newhouse also with the nickname, Chad and then CISO, Frank Armen, the CEO, Bruce Boyle the CFO, Jenny Cruickshank and deputy to CEO, Sara and a cyber security consultant Jack Parem. So basically the case study, it starts with a scenario where the Chad, the CEO of the company, he had just wired $ 49,999 to a someone, unknown person because the company has, is a victim of a ransomware attack and the hackers, they have actually gained access to the company's system and they have demonstrated the shutdown of one of the temperature control critical device and they also claim that they have accessed to certain sensitive recipe files of the organization and on the advice of his legal lawyer, the CEO has paid the ransomware to the attackers.

Now the case, this the current scenario is about a meeting which is taking place between the top executives and the CEO, Chad is really in a very angry mood and all the top executives, they are not able to make eye contact with him. " So what do we do?" ," Yes Mr. Chad I have been seeing some new intrusion monitoring systems on the market, I suggest we increase the budget for them and also we have to review our incident response protocol because SCC will come knocking to see our plans and procedures." So how much we have already spent on the system?" " About 6 million dollars." " 6 million dollars and still the breaches have increased.

" So now there is an uncomfortable silence in the meeting room and then you know, all of a sudden a lady voice that comes from the back of the room and she is actually Sara, the deputy to the CEO. " So why are our system even online? Shouldn't family recipes just be locked up on a paper? Why do we need them digitally and the pasteurization equipment and all?" So Sara briefed all the meeting heads about a new risk management process that she had read. It stated that the overly complicated software system are making organization more vulnerable to such attacks and it is not only the software system but also the anywhere and anytime access to the critical system of the organization. Many consultants recommend that the organization should put the humans back into the process and reduce the digitization. Now again this scene actually, shifts three weeks after that prior crisis meeting and on a workstation, the CEO and Frank the CISO and Sara, they are on the workstation and there is a fourth guy, the cyber security consultant, Jack Parem.

" Mr. Jack as you can see, the sensors in our tank send us real time data about everything. It tells us about our impurities, our temperature and bacteria, bacteria content. It saved us millions of dollars." "And the system is networked?" " Of course, otherwise we have to be in person monitoring the systems always.

So if anything goes out of order, we will get alerts. So this is very crucial to our cost savings." " And who has the access to the system?" " Basically it is anyone with a login. We usually give it to two or three people. Mostly it is me.

Last time I even logged into the system from my hotel." So the process continued for three weeks. In the process, the tech guy revisited all the processes of the factories and understood how the processes work. He mostly followed a four step plan. The first step was identifying the most critical information and the processes.

He visited each process, talked to the stakeholders and understood how the process exactly works. The second step was mapping the digital terrain in which those processes rested. It consisted of understanding the hardware and software part of the system. Also how the network is structured. And not only about the technology, it also involved understanding how humans are interacting in the system, understanding the supply chain and everything.

Third step, it was the most important step. In this step, the inputs from the first step and the second step were used and the most critical, likely part of the attack was identified based on the criticality and the openness of the system. In the fourth step, they generated, the options, about the attack based on the criticality, the attack which is most likely to happen and how critical it is. And during the steps of the evaluation, we can see

that Jack and every senior executive have undergone various intensive process of understanding the system. So, they were already exhausted and the kind of, they got an insight, like how they were really into digitization, that like, how much deep they have invested into the digital networks.

So, from the consultant's perspective, he found three points of failure. And he, he briefly sorted out into three categories, three are outcomes. In the first one is he found four pathways into the network and a hacker access industrial control systems. And the third one is one system was compromised by bot. And further his recommendations was that, first one he evaluated the thermization process which he advised the them, to take it completely offline and completely offline.

And then the second process was he advised them to remove the, the network controls, network temperature controls and automatic automated temperature adjustments or the other option was to keep them or and backstop them with human manual controls. And the third one, he found that during the penetration testing done by himself, he found that he was able to take control of the access control, he was taken control of the control systems and was also able to access all all of their recipes which was a huge eye opener to Chad. He was especially very shocked to know about, that his recipes could be accessible which could really hit this bottom line. So, we see that in the meeting a very heated discussion and debate takes place on the various suggestion offered by the cyber security consultant. "So whole point of going digital was to save money, going offline would kill the bottom line.

" " Look Mr. Bruce, the goal is not to take back to your stone age, it just to reduce your digital pathways. The most likely vectors that any attack could possibly happen. So, even so, even though there is very likelihood of attacks. So, I would really suggest to you to look back, look at the situation here and and make corrections." "So, you want us to roll back the business 20 years, for a one in a million chance.

" " Look Frank, I came here because you were attacked by a ransomware, but frankly ransomware does not scare me, listeria does. If you check recent health hazards created by companies, you can really see the consequences of a major catastrophe. So, it could really affect every company." So, just to give an idea about a ransomware and how it works, basically the hacker or the bad guy, either he creates the ransomware himself or he can buy atleast from the cyber criminals. In fact you will be surprised now a days there is something called as RAS, ransomware as a service, they are business models and they are creating and selling all these ransomware software to the criminals.

And after that the cyber criminals basically exploit the social engineering skills and all

and then he enters the access to the system and he encrypts the IT system and the data whatever possible. And basically the main intention is to you know, ask for the money, ransom and at times they ask in a cryptocurrency form also. So the audience, we would like to know your opinion - Should Chad implement consultant's recommendation? The consultant's input is that we take most critical parts of the value chain off the digital environment for protection and we do not essentially move back 20 years, that we remove all of digitalization or digitization which has been built in. So, this the, this is an in between solution which will ensure that some form of optimization is obtained through the digitization process but at the same time, the critical assets are protected. So, it could be in my opinion good to move in that direction, identify which are the most critical assets and move them offline.

Anyone, any other suggestions? They should go ahead with that and we had already covered regarding this, we had there was a presentation also that was that Cyber Informed Engineering which basically says that your critical systems should have a contingency plan already mapped out and so that anytime such a thing happens, you can always as far as possible, try to keep them out of the digital connectivity loop. so that nobody can attack them. So, yes definitely that particular concept works out very well and will continue to work out well in the near future also. Yeah, even I would suggest an in between solution because going completely offline might not be that useful because for example, the sensors might be tracking the temperature and all and we might need the help of IoT to track those changes and you know for the predictive maintenance of the machine that are being employed, it will help in increasing the efficiency of the system in the long term. So, completely moving offline just for the cyber security risk sake might not be a fruitful option in the long term.

So, but just as sir mentioned we can identify the critical aspects of the business and then just move them alone offline or just restrict the access within the local environment or something like that can be pursued. Okay, I have a question, If you go back or roll back the system to manual controls, can there still be manual errors because when human beings control temperature or monitor temperature, you are trusting human beings and that is why you go for automation because human beings, human errors are quite possible. So, you go for automation and in automation you have other problems created by humans. So, do you see the solution as going back or something else because human errors can still happen. Yes Sir, you are right Sir, in fact the errors can be there, in fact the earlier when the company was, had not digitalized, they were facing lot of problems, there were lot of wastages were there because the human error and all and that was the purpose they went for digitalization and just for the sake of that actually we have displayed some of the pros and cons.

So, in case the company goes for a mix, you know, system of manual and combination of the digital. So, certain pros are there actually. Yeah, obviously like the first one in case of pros, obviously there will be isolation and prevention of the critical system. So that there is a least damage. So, we have something called as you know, theory of least privileges.

So, in case someone access to that so he is not able to access the in totality or the complete system or so that he access only the compartmentalization is there. Again, in case the second point what we have displayed here that the production, in case someone accesses, the attacker. So, the complete production may not be hindered some of the manual system may still be as a backup or as a parallel system, they still will be working. And thirdly the sensitive data that is more secured in offline mode because we might be having trustful and faithful employees, obviously that can be debatable again as you said Sir. And fourthly there might be less chances of unauthorized access, that will obviously be there but yeah, that chances can be reduced.

Again coming on to the some of the cons. Since firstly the company has done lot of investment in terms of money in the automation and digitalization. So now again reverting back to the manual mode. So, it is all on the cost of that automation and money spent, it is something like a sunken cost, that money has already been spent. And secondly yeah, the investors once they will come to know about this thing that might affect the reputation of the company and the trust you know, in the mind of investors and public.

And thirdly, obviously the raised cost might be there because they have to hire faithful employees and train them and this skill enhancement that is required. And fourthly during the initial stage actually, this setting up of the parallel system, there might be some hindrance to the operations, that will obviously be there. Yeah. So, this case as you presented illustrates the cyber security challenges to the industry, particularly industrial automation when it is going towards IoT devices industry 4.

0. There are lot of pluses as you showed and there are also risk and major risk which can create financial loss but also, as you pointed out, loss to lives you know listeria, where it is about changing the composition of a food product. You know if you consume that product which is actually got produced not following the standards, then you are eating something which is, you do not know you can die, if you eat that product. So, the kind of consequence that if industrial controls are affected by cyber attackers is very, very high and severe. And also, you see this case highlights the ransomware attack. So, already there have been major ransomware attacks like the WannaCry, NotPetya which happened at the country level.

It is like you know, the WannaCry was possibly done by North Korea and NotPetya by Russia. So, this is also part of cyber attacks at a national level. I did not know for sure but these are actually observations in reports. So, they say NotPetya case, they actually encrypted your machines and they asked for ransom but even if you pay the ransom, they did not release the machines. So, in this case it says, you have to pay $49,999 and your machine is released.

And if that happens it is fine, you can go on but if as in the case of NotPetya, if they do not release the machine even after making the payment, it is like killing your systems. So, the consequence of ransomware which is very much highlighted in this case, is very high at the moment and in terms of threat intelligence, that is a very high threat in today's world particularly in industrial controls. And solutions are still evolving you showed some of them and let us move on with risk management in the next session also. And in the next session of course, you have someone from industry coming in, perhaps you get more insights.