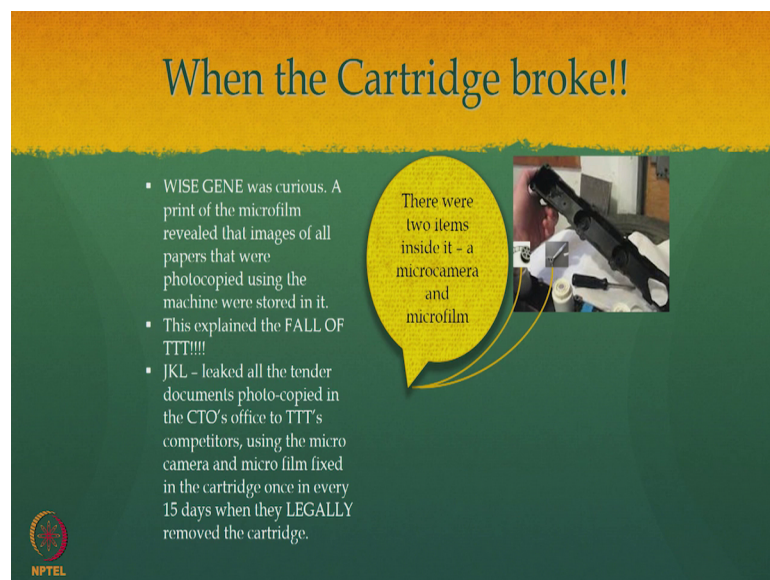


Information Security - IV
Prof. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 02
WISE GEN and The IT Revolution* - 1

Welcome to session two. So, last time, last session, we actually stop with my heroine wise gen actually pulling out the cartridge, and the cartridge fell down and it fell and it broke.


(Refer Slide Time: 00:25)




When the Cartridge broke!!

- WISE GENE was curious. A print of the microfilm revealed that images of all papers that were photocopied using the machine were stored in it.
- This explained the FALL OF TTT!!!!
- JKL - leaked all the tender documents photo-copied in the CTO's office to TTT's competitors, using the micro camera and micro film fixed in the cartridge once in every 15 days when they LEGALLY removed the cartridge.

There were two items inside it - a microcamera and microfilm





When it broke see here on the slide, there were two items inside it. She actually wind a micro camera and then a micro film that is pro protruding out of this. She is wise; my heroine is very wise. So, she immediately was able to relate the entire thing. So, what has happened every 15 days the JKL fellow took the cartridge out, and it took the microfilm from the micro camera and the made a print of this what was there in the film. So, what was there inside the film, every paper that was photo copied in the last 15 days a image of that was stored in the micro camera. And when they open the micro ca[amera] when the micro camera was taken out, and they made a print out all the documents for printer, so that included the tender documents also the quotations also.

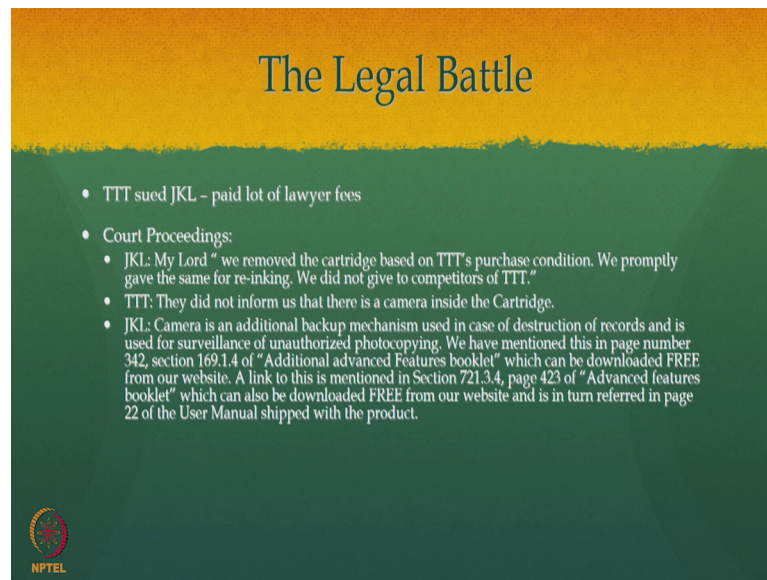
So, basically JKL got access to all these documents which included the quotation, and obviously, he shared it to the competitors. The competitors when they looked at this

quotation they know the exact pricing that this fellows have quoted and so they quoted something like one rupee less. So, you quote for 105 rupees, he will quote for 104 rupees 99 paisa , and he was getting the tender right. And this explained completely how why JKL TTT the company lost their entire game.

Now, what was wrong here, was it the people, was it the process, was it the technology? Lot of process was followed to buy this machine. Whom should blame here, what happened right? So, let us start doing a forensic of how do how this has happened and what we would we could have done to prevent it. So, one of the thing is that this something somebody gives you free, see if somebody comes and tells I will give you a cartridge free every 15 days , the company should have been a fool to not suspect it right. So, if something is given as a discount, we should take it with the pinch of salt. If you are a if you really want to build a career in security, this is the first advice you should give if you have called as a security consultant, anything given free, take it with a pinch of salt, this is one very interesting example there.

Now, this was obvious, so you immediately TTT actually went and sued, JKL saying this is a and paid lot of lawyer fees ok, because it is a very high technical case. Even if it is not, it will be made one because the way we can get a proof for this is really going to be technical not going to be easy. Though, the problem is very simple it really becomes a in a very big case technically so solid case. And we need really powerful lawyers to argue this case in the court, but this case could did not even could not even survive in favour of JKL for the simple reason.

(Refer Slide Time: 03:19)



The Legal Battle

- TTT sued JKL - paid lot of lawyer fees
- Court Proceedings:
 - JKL: My Lord " we removed the cartridge based on TTT's purchase condition. We promptly gave the same for re-inking. We did not give to competitors of TTT."
 - TTT: They did not inform us that there is a camera inside the Cartridge.
 - JKL: Camera is an additional backup mechanism used in case of destruction of records and is used for surveillance of unauthorized photocopying. We have mentioned this in page number 342, section 169.1.4 of "Additional advanced Features booklet" which can be downloaded FREE from our website. A link to this is mentioned in Section 721.3.4, page 423 of "Advanced features booklet" which can also be downloaded FREE from our website and is in turn referred in page 22 of the User Manual shipped with the product.

NPTEL

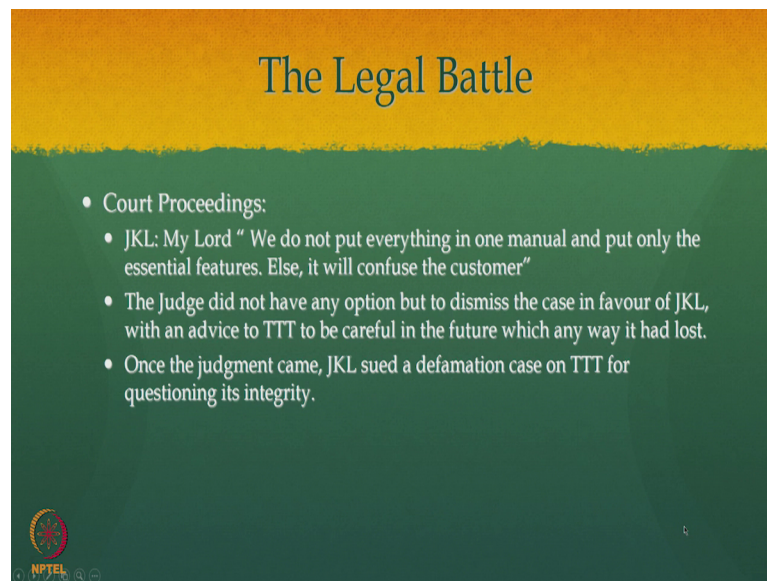
So, JKL went and told My Lord., we remove the cartridge based on TTT's purchase condition. Now, TTT went inside that they had a camera inside, and they removed. The JKL told I removed it because you have you give a purchase order the TTT as a company has given me a purchase order. They told me I have to remove every 15 days, I removed it based on them. They even set a process, I could go in everybody was watching. I removed the cartridge, put a new cartridge. I get took it back; i it completely re-inked it and give it to a school. I am a reseller somebody makes this. I am ask to do this; I did it. I do not do anything more than this is this is what JKL says.

Now, TTT went back and said this and that did not inform as the there is a camera inside the cartridge. So, this fellow also said immediately, JKL also said they did not also ask what ink I am using. So, I need not explain everything. Please note, this is something very important, JKL's argument, the last part of this slide. Camera is an additional backup mechanism used in case of destruction of records and is used for surveillance of unauthorised photocopy that is the reason why I have kept a camera inside. We have mentioned this in page number 342 section 169.1.4 of Additional advanced Features booklet which can be downloaded FREE from our website.

When you bought this you should have download all those things and seeing what is inside. A link to this is mentioned in section 721.3.4, page 423 of Advanced features booklet which can also be downloaded FREE from our website and is in turn referred in

page 22 of the User Manual which are shipped with the product. So, you should have read the user manual, there was a pointer there. You should have gone and read that entire document; in that there was type pointer, from that you should have go and read another document and you are really found out that there is a camera right. So, do not say that I did not inform you, this is all there.

(Refer Slide Time: 05:30)



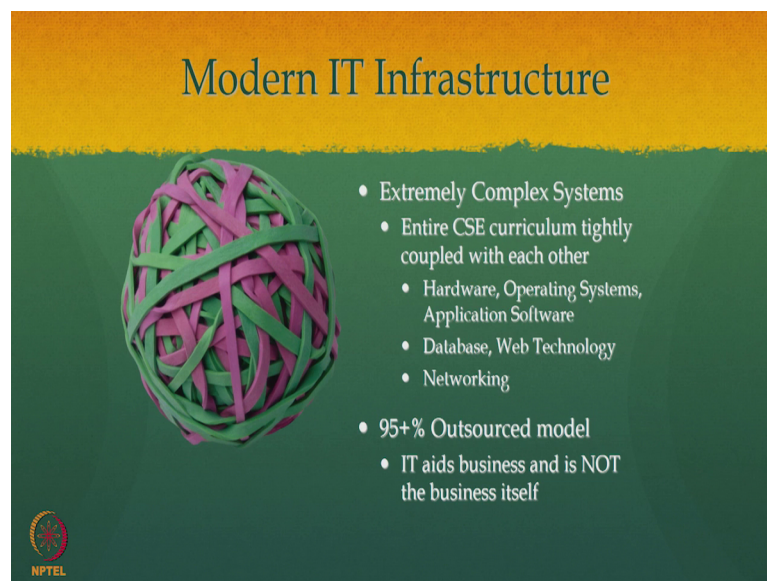
It is also went again and said. So, JKL said we do not put everything, so we just put something very interesting and important. So, so do not expect us to put everything when it will confuse customer. So, when this argument was proved that yes there is it is because the company TTT did not go through the thousand page manual related to an Xerox machine or a photocopier machine, it is their mistake. They should have gone through. Ladies and gentlemen, whenever you say I agree right, whenever install a software you say I agree, somewhere you say there is license condition you say I agree right, many of the industries sign service level agreement without understanding the technical aspects right.

So, please be very careful when you are doing this right. Because when you press that I agree, you are legally bounded by what that means now coming back the judge did not have any option, but to dismiss the case in favour of the photocopier machine companies JKL with an advice to TTT to be careful in the future which any way it had lost.

So, once judgement came, this is interesting JKL sued a defamation case on TTT for questioning its integrity right. So, this is a cyber fraud which has happened where you cannot trace back, there is no forensic that you can do, there is no proof that JKL as indeed removed the camera, improve removed slides, removed the film he made a copy; even if he made a copy, he shared it with the competitor nothing could be proved here because as the cartridge leaves out your premises, it is completely in the custody of the JKL.

Your purchase condition says that once he replaced the replaced cartridge right, the cartridge that has been removed, and it has been replaced by new one, they removed cartridge moment this exchange happen is the property of the JKL. So, I do not know legally whether you can sue or not. So, this is a very interesting question. I hope some lawyers see this course, and they can make a decision about that.

(Refer Slide Time: 07:53)



Modern IT Infrastructure

- Extremely Complex Systems
 - Entire CSE curriculum tightly coupled with each other
 - Hardware, Operating Systems, Application Software
 - Database, Web Technology
 - Networking
- 95+% Outsourced model
 - IT aids business and is NOT the business itself

NPTEL

So, what happened next. So, just to basically tell you one thing that modern IT infrastructure is extremely complex system. We are just talked about one simple photocopy machine right. But if you really take any infrastructure, let us take a financial institution like a bank there is a data centre. Inside the data centre, what are the things you we have we have a database first, where your account number everything is stored, all the details about transactions are stored. Then there is going to be an huge setup server which are doing your web application to access this database there are there will

be an operating system on which these servers are running. There will be a networking which connects all this with external world and also internally both the LAN and WAN networking.

So, at least four important components, the hardware, the software, the operating system, the web application web database networking at least these are all five different courses in CSE curriculum. Any curriculum across the world in computer science engineering undergraduate or postgraduate under graduate in specific will have whatever I mention database, networking, hardware, software, operating system, these are all fundamental core courses in this

So, for me to have a global understanding, because even look at a fraud right, it is not going to be just on the operating system it can be a combination of vulnerabilities that existed in the network plus operating system, network plus operating system plus hardware. So, where the vulnerabilities comes, how it come these are all questions that need to be answered in a very, very big way. For me to have a complete version of this, I need to be sort of you know aware of all the entities.

The entire CSE curriculum the computer science and engineering curriculum, all the systems courses, I should be thorough enough for me to understand what is happening inside a data centre. Not only the understanding of that when something that is not to happen has happened then going and doing and forensic will need very deep understanding of not only cursory level, but very deep understanding of the functioning of the hardware, the data base, the web application, the operating system and the networking right.

And today when we look at IT infrastructure say financial institution, insurance institutions, many, many things like you know factories etcetera these are all outsourced models. Some system integrator maintains it for you and gives you the service. So, in the case of cyber forensic attack that is happened , what is the insight a particular organisation will have, all the insights have to come to the system integrator, they are not going to have an insight. It is very difficult for an organisation to have an independent insight of this and that is also another major issue. So, do I own, yes, IT infrastructure yes, but do I govern that IT infrastructure largely no, 95 percent of this is basically you

know taken off from you know from the outsource model. Somebody else maintenance it and you just use it. So, this is how the modern IT infrastructure works.

So, this is one story that I want to tell as a part of session two. Now, in the next session, I will know elaborate. So, WISE Gen moved out to some other industries because she lost the job and the Xerox machine also failed, so now she actually moved into another industry and then we will start tracing her career from that industry onwards in the next session.

Thank you.