

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

Lecture- 01
Introduction WISE Gen and The IT Revolution- 1

[FL] welcome to information security IV. This is the 4th in the series of the 3 courses that we had offered earlier, the first one basically introduced you to all the notations terminologies of the entire game of information security starting from hardware, architecture, software, compilers and then network etcetera.

The second course actually dealt with some of the hardware features that are available for you to build a secure system. The third course introduced you to different face such of operating systems and networking; which are the foundation building blocks for understanding security at these levels. Now in the 4th course we are now going to deal with something which is very important and interesting which is 4 and 6 of information security attacks.

What we will be covering is that we will be giving you some case studies of some of the information security attacks that had happened and, but importantly we will cover some of the details; that will make you quite proficient with understanding the system and the networking in detail that will enable you to do 4 and 6 in a logical directed way. Any information security system today needs to be protected and in case of an attack should provide enough information for us to go and trace out what has happened.

So, in the direction it needs to be monitored also. So, there are 2 facets in building any information security infrastructure, the first part is to see that necessary security is ensured, the second part is that in case of there is an attack how do we go and what are the traces what are the facilities that are available for us to do an analysis or investigation which we call as forensics to come out and find out what exactly happened during that attack; both are extremely important and the first 3 courses basically thought you more about building secure systems, the 4th course actually talks about how to fine tune or how to model your infrastructure in such a way that you can do sensible forensic in the case of an attack.

In this couple of sessions that I will be handling I am basically going to talk about how attacks basically originate. What are the types of attacks? I give you some a list of examples, the weakest link how does an attack happen. The attack actually happens because there is an issue at one of the 3 levels; I think these 3 levels we have been continuously mentioning in the last 3 information security courses under the same in n p t e l platform.

The 3 important things that govern a security of the system is people followed by process followed by technology. If the end user namely the people they are weak then certainly, the technology whatever good technology you have you may have; the best password encryption algorithm, you may have the best supervisor permission in the operating system that nobody could go and tamper these confidential thing, but if somebody is going to basically put their password in Facebook or stick it on a notice board, then whatever be the encryption algorithm whatever be the other thing you cannot do anything about it right.

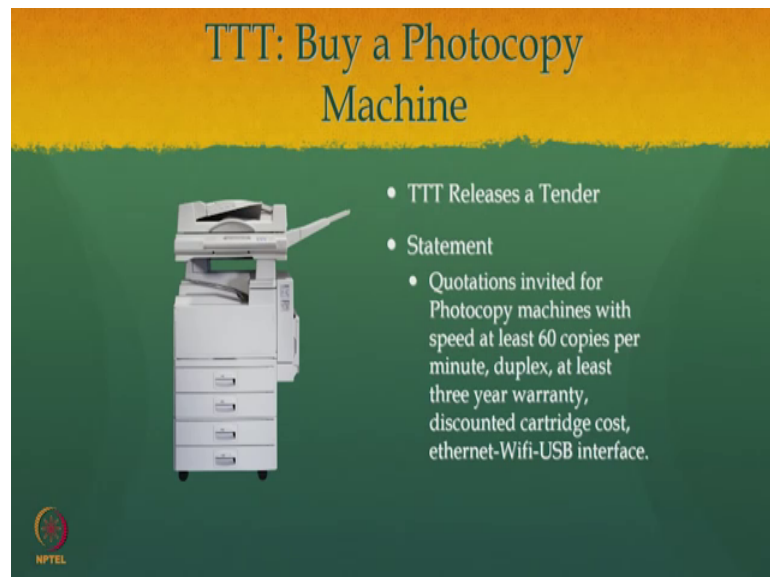
So, the entire system becomes extremely weak if the end users are not sensitized to the basic principles of security. So, that is why the government of India has a program called information security education awareness program the IACA, the prime objective of this program sponsored by the ministry ministry of information technology under whose auspices these course materials have been developed is to go and spread this awareness about information security. So, that main concentration that is that people of different walks of life need to basically understand what is security. The second aspect is about the process, how do you ensure security? So, if there is something wrong in the process, where then the information can leak and a third is of course, technology and it is also also in the same order people process and technology .

So, so we have to strengthen all these aspects. So, when we look at forensic we should have a holistic way of looking at people, then I have to look at process, then I have to look start looking at technology. And all these 3 things are very important and now what we will do in the first 3 sessions; is I am going to talk about some of the prominent attacks or information security leaks that had happened ah. And how what would be the reaction to that so where do we blame, is it the people that we are going to blame on the process of the technology, we will have a clear analysis and that is what we are going to do in the first 4 to 5 sessions .

This first couple of sessions I want to start with a story , in this story there is a heroid wise gen and what I am just you know going to tell the story where I am going to trace the carrier path of wise gen right? And then in the IT ah revolution that is happening. And then all the attacks that had happened I am going to fit into her carrier and tell how these attacks have happened and this is the story that I am going to tell in the next 3 to 4 sessions.

Now, welcome to this session this is wise gen and the IT revolution and I am professor Kamakoti of I I T madras and this is the first screen ok.

(Refer Slide Time: 06:14).

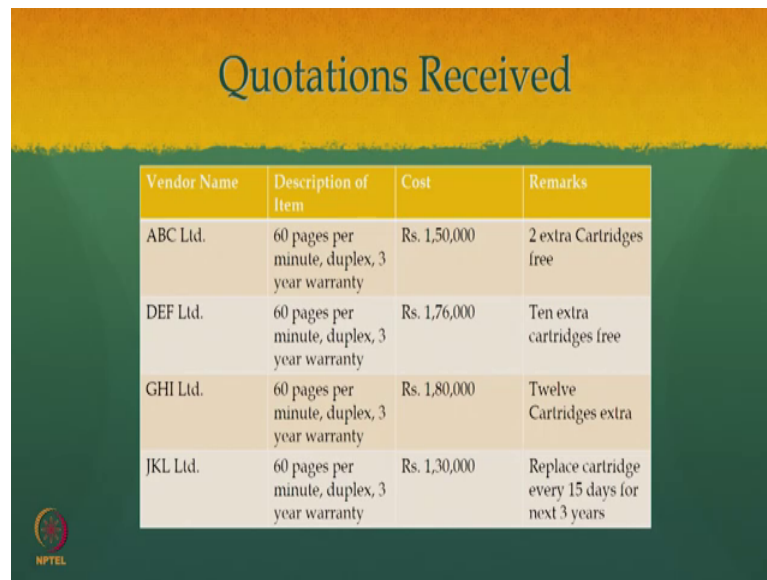


The slide features a yellow header with the title "TTT: Buy a Photocopy Machine" in a serif font. Below the title is a large, white, multi-tiered photocopier. To the right of the copier is a bulleted list of requirements. In the bottom left corner, there is a small circular logo with the text "NPTEL" below it.

- TTT Releases a Tender
- Statement
 - Quotations invited for Photocopy machines with speed at least 60 copies per minute, duplex, at least three year warranty, discounted cartridge cost, ethernet-Wifi-USB interface.

Now the story starts with a company named in TTT, who wants to buy a photocopy machine right. So, they release a tender inviting you know quotations and the statement in the tender was that we need photocopy machines which speed at least the 60 copies per minute, it should have duplex it should have at least 3-year warranty and then discounted cartridge cost then all the other interfaces like I should be able to connect to the printer or the photocopy machine by internet, Wi-Fi, USB interface etcetera.

(Refer Slide Time: 06:41).



Vendor Name	Description of Item	Cost	Remarks
ABC Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,50,000	2 extra Cartridges free
DEF Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,76,000	Ten extra cartridges free
GHI Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,80,000	Twelve Cartridges extra
JKL Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,30,000	Replace cartridge every 15 days for next 3 years

These were the quotations is a 4 companies coated against the tender and everybody said that they can give 60 pages per minute, they can say they said they have duplex they will give you 3-year warranty; no problem and then there were the castings 1 2 3 4 5 and then they were asking like discount at cartridge cost right.

So, that was a very intelligent thing that was put in the tender ah; it was basically learned from the process that the cartridge cost much more than the printer right. Or the cartridge cost much more than the photocopy machine vocalized-noise] right? In over all the amount of money you spent on a recurring basis to buy cartridges would very soon exceed the cost of the printer of the photocopy machine.

So, that is why they are asked for discounted cartridges very Intel, very important part of the tender. And there you see that there are the first fellow ABC set I will give you 2 extra cartridges, the second fellow said I will give 10 extra cartridges free, well the third fellow said I will give you 12 the 4th fellow set that he will not give anything free extra, but you will replace every 15 days you will replace a cartridge for the next 2 3 years free of cost.

(Refer Slide Time: 07:54)

Tender Opening

- The Purchase Committee
 - **Technical committee** - Machine is an elephant - cartridge is the food to it. The latter costs heavily.
 - **Finance Committee** - Recurring expenditure is very high and we have to somehow bring it under control.

Vendor Name	Description of Item	Cost	Remarks
ABC Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,50,000	2 extra Cartridges free
DEF Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,76,000	Ten extra cartridges free
GHI Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,80,000	Twelve Cartridges extra
JKL Ltd.	60 pages per minute, duplex, 3 year warranty	Rs. 1,30,000	Replace cartridge every 15 days for next 3 years

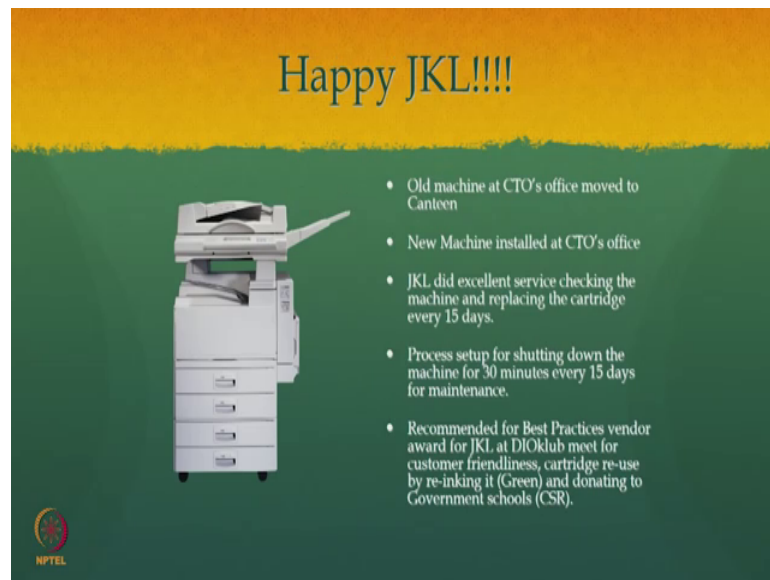
Decision: BUY from JKL



So, this was this was the tender and; obviously, the purchase committee met the process is followed here please understand , and the technical committee open suing all these tender a machine is one thing, but cartridge is going to be the recurring his expenditure. So, machine is like an elephant that you pick only one purchase, but cartridge is the food you give to the elephant. So, you meet repeated purchase of that food and that is going to become much costly. When the finance committee said that recurring expenditure is more higher than the capital expenditure and cartridges are recurring expenditures.


So, let us go on so so based on all these things it was an obvious choice by these committees to go in for JKL, who had quoted the least one lakh 30 thousand from this photocopy machine and he also said that he will replace the cartridge every 15 days for the next 3 years.

(Refer Slide Time: 08:40).



Happy JKL!!!!

- Old machine at CTO's office moved to Canteen
- New Machine installed at CTO's office
- JKL did excellent service checking the machine and replacing the cartridge every 15 days.
- Process setup for shutting down the machine for 30 minutes every 15 days for maintenance.
- Recommended for Best Practices vendor award for JKL at DIOkub meet for customer friendliness, cartridge re-use by re-inking it (Green) and donating to Government schools (CSR).

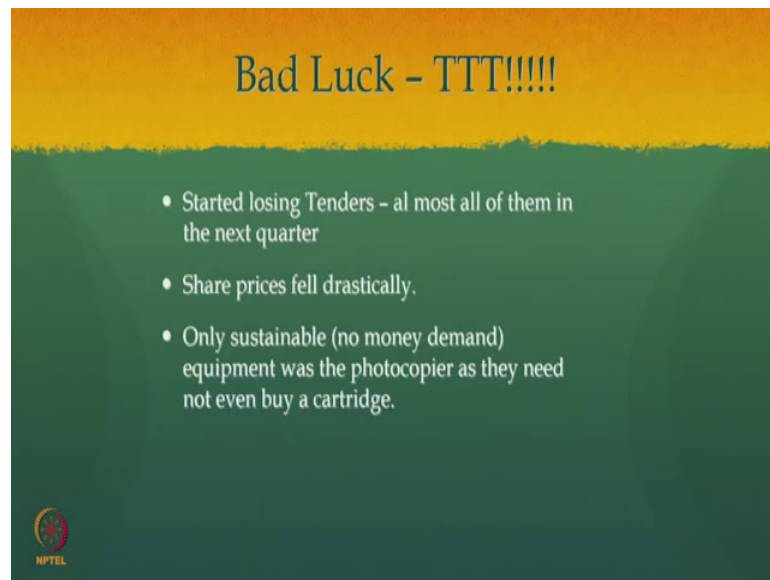


So, the JKL was extremely happy so he really wanted this order so he got this. And then what happened. So, the new photocopier machine was delivered it is quite obvious that the old machine which was in the CTO office for which this replacement was to be made was moved to the canteen; just started Xeroxing all these tiffin bills; well this new machine was got installed in CTO office which is also correct way the process right.

And JKL did excellent because his first order he had to really catch the market. So, maybe say a company as you see. So, he did excellent service every 15 days promptly came he replaced the cartridge took the older cartridge put the new cartridge and things went off very fine. It went to an extent that there was a process again set up that every 15 days this photocopier machine will be stopped JKL will come he will remove that old the cartridge put the new cartridge and then go.


So, there was a definite shutdown period for this photocopier machine for usage every 15 days. So, taken was doing it was doing excellent customer service then he took this cartridge re inked it. So, he was doing green service then this re inked cartridge he was giving to some government schools. So, it was doing social service. So, JKL was awarded the best vendor award because he was doing good customer service. He was quite aware of green initiatives and he was also doing lot of cartridge social responsibility. So, he was given a very good award for all this stuff the.

(Refer Slide Time: 10:08).



Bad Luck - TTT!!!!

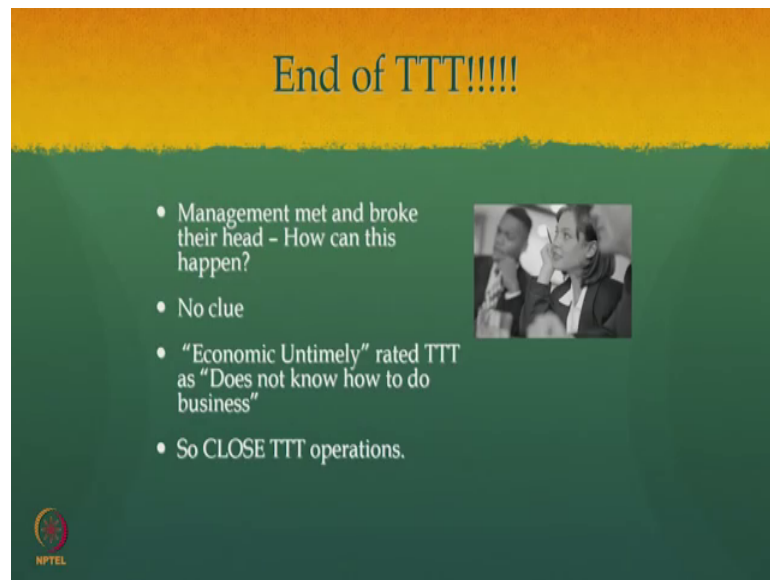
- Started losing Tenders - almost all of them in the next quarter
- Share prices fell drastically.
- Only sustainable (no money demand) equipment was the photocopier as they need not even buy a cartridge.

 NPTEL

Things were fine going on, but suddenly what happened TTT the company which purchased this photocopy machine started losing tenders. Almost all of them they lost in the next quarter everything they could somebody could do better than them and they take the order.



So, when they did not get any order in the last 6 months immediately, the share prices started falling drastically. So, at this point there was no income and there is a lot of expenditure. So, the only sustainable thing interestingly was this photocopy machine because they were you know this was under annual maintenance and every 15 days that company JKL was coming and replacing the cartridge. So, it was not incurring any expenditure and it was well maintained it was quite.

(Refer Slide Time: 10:59).



End of TTT!!!!

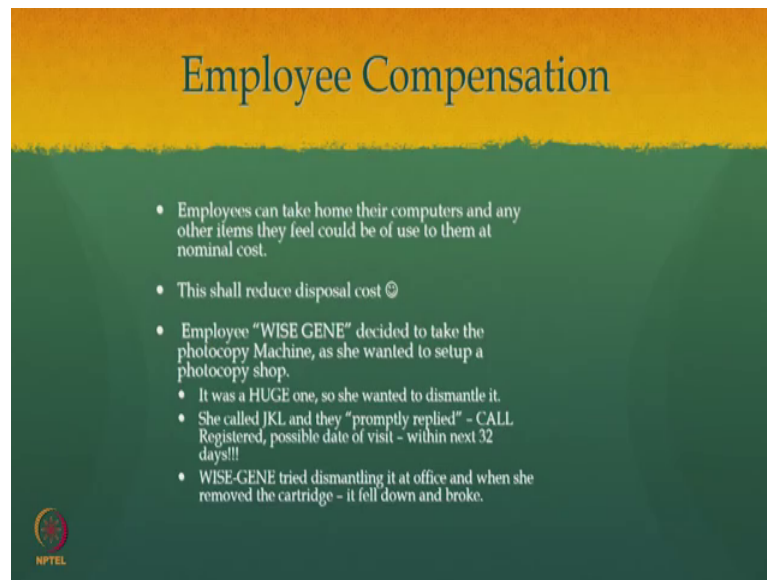
- Management met and broke their head - How can this happen?
- No clue
- "Economic Untimely" rated TTT as "Does not know how to do business"
- So CLOSE TTT operations.



So, since these share prices fell the company was in real doldrums; then the actually the management met they broke their head, they found what happened their country even could one tender properly they did not any good. So, they went through all the process how people arrived at tender values everything they had been doing this for years together and they had been extremely successful suddenly.

No clue where they are using in then lot of magazines like economic untimely rated TTT as does not know how to do business and then finally, the management that is decided to close TTT operations so this is the status.

(Refer Slide Time: 11:34).



The slide features a title 'Employee Compensation' in a serif font at the top. Below the title is a list of five bullet points. The first two points are general statements about employee take-home items and disposal costs. The third point is a specific anecdote about an employee named 'WISE GENE' who took a photocopier home. The fourth and fifth points are sub-bullets detailing the employee's actions and the resulting issues. In the bottom left corner, there is a small circular logo with the text 'NPTEL' underneath it.

- Employees can take home their computers and any other items they feel could be of use to them at nominal cost.
- This shall reduce disposal cost ☺
- Employee "WISE GENE" decided to take the photocopier Machine, as she wanted to setup a photocopy shop.
 - It was a HUGE one, so she wanted to dismantle it.
 - She called JKL and they "promptly replied" - CALL Registered, possible date of visit - within next 32 days!!!
 - WISE-GENE tried dismantling it at office and when she removed the cartridge - it fell down and broke.

So, the main issue is that knowing we have an electronic hardware. We can not throughout that hardware purchasing the hardware, if you say has a difficulty level of x condemning that hardware has difficulty level of 10 x because electronic components will have lot of caustic materials chemicals.

So, there will be lot of environmental issue when you want to dump electronic conference. So, and there will be lot of money involved in recycling making it safe and then just you know giving it out. So, the company; obviously, said if there are working electronic components, they said all the employees anyway we are causing please take whatever you want you please take it home, please decide what you want and take it home ok. Because this will reduce the disposal cost which would be much more than the procurement cost many times.

So now comes my heroin wise genes is wise. So, she thought like we are losing the job let me take this photocopier machines a brand new one, I will put a photocopy shop rent a small place put a photocopy shop start earning some money from this and then try and talk to that company JKL if they can support this machine for some time and let us run this show.

So, she is started you know it was a very huge machine so she wanted to dismantle it for taking it home in may not to or something. So now, she called JKL and they JKL promptly replayed they can know that this company is closing. So, they promptly replied

call is registered possible data visit within next 32 days so; obviously, 32 days this company will not survive. So, wise gene said let me let me just open it up let me try and dismantle it , when wise gene tried and dismantled it at the office right.

So, he has to dismantle so first he removed the cartridge the cartridge fell down and it broke and that is where I am going to stop this session 1; with this story before you start looking at my next session session 2, try and find out what would have happened this cartridge break breaking I am just stopping it like a nice you know TV serial ok. So, this cartridge breaking and purchase of a Xerox machine plus JKL coming and replacing it every 15 days and then the company TTT closing it is operation all these 4 does it have something in common, can you relate it just think before you go and see my session 2 that is going to follow. I hope this is interesting I want all of you to start interacting with us.

There is a very interesting topic cyber forensic I want all of you to start interacting with us through the a portal there is a portal made available by the MOOC platform of IIT madras, where you can post your queries you can also say the lecture was interesting lecture was boring, you can also give all feedbacks right? You are interested in taking those feedbacks because as you know in in time to come we want to start refining these courses and make them more robust and more informative. So, I look for very active participation from your end in especially, the cyber forensic course we will meet you in session 2.