Case Discussion: Computer Crime

USPA & IRA Company

A former programmer in Fort Worth, Texas, has been convicted of planting a computer virus in his employer's system that wiped out 168,000 records and was activated like a time bomb, doing its damage two days after he was fired. Tarrant County Assistant District Attorney Davis McCown said he believes he is the first prosecutor in the country to convict someone for destroying computer records using a virus. Donald Gene Burleson, 40, was convicted of Charges of harmful access to a computer, a third-degree felony that carries up to 10 years in prison and up to $5,000 in fines. Burleson planted the virus in revenge for its firing from an insurance company, McCown said.

Jurors were told during a technical and sometimes complicated three-week trial that Burleson planted a rogue program in the computer system used to store records at USPA and IRA Co., a Fort Worth-based insurance and brokerage firm. The virus, McCown said, was activated two days after Burleson had been fired because of personality conflicts with other employees. "There were a series of programs built into the system as early as Labor Day," McCown said. Once he got fired, those programs went off. The virus was discovered two days later, after it had eliminated 168,000 payroll records, holding up company paychecks for more than a month.

Questions for discussion:

a. Why is "Donald Burleson virus attack" a crime? List the harms it did to the person, the employer and the society.

b. What social issues, in addition to crime, can be related to the case? And how?

(Employment, Social Application, Privacy, Competition, Quality of Life etc.)

c. Are there any individual issues, which caused the crime to occur?

(Ergonomics, Skill and Knowledge, Autonomy and Power, Scope of Work, Involvement and Commitment etc.)

d. What are ethical and legal issues involved with it?

e. Suggest the way the crime could have been stopped.

*(**Note:** the questions may be distributed among groups for discussion.)*

Issues and Discussions:

Summary of discussions in BEIT, NCIT

It is a crime because

- it was a deed that is against the law
- it seized the employees' right to get salary for a month
- it resulted in the loss of data and information (it wiped out 168,000 records)
- it had made malicious access to corporate data

It did harm the person individually in the following ways:

- Burleson, the programmer, had to pay $5,000 as a fine and 10 years of imprisonment.
- He developed bad impression in the organization and the society
- There was negative impact in his career.
- He had to bear mental torture also

It did harm the employer in the following ways:

- It affected the Payroll management
- Extra efforts, time and resources needed to be paid in recovering from the disaster
- Misunderstanding among the employees could be created
- Security of the system of the organization was challenged.

It did harm to the society in the following ways:

- The dependents of the employees were affected for a month because they did not get paid
- Could have established a bad impression in the society and the credibility of the company could have become an issue
- Could be a source for committing such crime for others in the society too.

There seemed to have following Social and Individual aspects involved in the case:

- Personal conflict between the programmer and his employer (?)
- Work environment of the company
- Unhealthy competition, ego, revenge etc developed in the company
- Quality of life of the programmer
- Attitude of the person
- Skill and knowledge of Burleson
- Autonomy and Power given to him
- Scope of Work of the criminal
- Level of Involvement in the work and level of Commitment to the organization

There are some legal and ethical issues, too, in the case and they are:

- Burleson should not be fired just because of the personal conflict.
- He, the programmer should not take revenge to the whole organization
- Destroying information of the company is illegal and making employees payless is unethical.

Different attempts could have been carried out to prevent from such crimes well in advance or safety measures could have been taken to recover from the disaster such as:

- Physical and data security of the information
- Regular data backup
- Conflict resolution of the programmer and the employer
- Strict enforcement of rules and regulations of the company.

References for the discussion

What is a computer crime?

Computer crime is defined by the laws and the current legislations, which is different for different nations and also may change at different times.

The Data Processing Management Association **(DPMA)** defines computer crime more specifically. Its Model Computer Crime Act defines computer crime as

(1) the unauthorized use, access, modification, and destruction of hardware, software, or data resources,

(2) the unauthorized release of information,

(3) the unauthorized copying of software,

(4) denying an end user access to his or her own hardware, software or data resources,

(5) using or conspiring to use computer resources to commit a felony

(6) the *intent* to illegally obtain information or tangible property through the use of computers, and

(7) the *intent* to establish control for the purpose of unauthorized experimentation with computer resources.

Types of Crime (examples): -

- Money theft
- Computer viruses
- Service theft
- Program and data theft
- Program copying
- Data alteration
- Program damage
- Data destruction
- Malicious access
- Violation of Privacy
- Violation of International Law