ASSIGNMENT #4

Q.1. Why is “Donald Burleson virus attack” a crime? List the harms it did to the person, the employer and the society.

Ans. The "Donald Burleson virus attack" is a crime because it involves unauthorized access to and malicious manipulation of computer systems, resulting in significant damage to data and disruption of operations. Burleson's actions violated laws that protect computer systems and data integrity, specifically those concerning harmful access to computers and the intentional infliction of harm.

Harms to the Person:

1. **Burleson:** Conviction led to severe legal consequences, including potential imprisonment and fines, damaging his personal and professional reputation.
2. **Other Employees:** Payroll disruption affected their financial stability, causing stress and potential financial hardship.

Harms to the Employer:

1. **Data Loss:** The deletion of 168,000 payroll records caused substantial operational disruption.
2. **Financial Impact:** The company faced delayed payroll, possibly leading to financial penalties, loss of trust, and increased costs to restore data.
3. **Reputation Damage:** The attack likely damaged the company’s reputation, affecting its relationships with employees, clients, and stakeholders.

Harms to Society:

1. **Economic Disruption:** Such attacks can disrupt local economies and erode trust in digital systems.
2. **Security Concerns:** The incident highlighted vulnerabilities in computer systems, raising broader concerns about cybersecurity.
3. **Precedent:** It sets a troubling precedent that disgruntled employees might resort to similar actions, potentially increasing such crimes.

Q.2. What social issues, in addition to crime, can be related to the case? And how?

Ans.

Employment Practices:

- **Workplace Culture:** Personality conflicts and toxic work environments can lead to extreme responses. The case underscores the importance of healthy workplace relationships and conflict resolution mechanisms.
- **Employee Support:** Lack of support for terminated employees, such as counseling or transition assistance, might lead to retaliatory actions.

Cybersecurity Awareness:

- **Insider Threats:** The case highlights the risk of insider threats, emphasizing the need for robust cybersecurity measures to prevent internal attacks.
- **Training and Education:** Organizations must educate employees about ethical behavior and the legal consequences of cybercrimes.

Q.3. Are there any individual issues, which caused the crime to occur?

Ans.

Personal Grievances:

- Burleson's actions were driven by personal grievances stemming from personality conflicts and his firing. Feelings of unfair treatment or revenge can lead to destructive behavior.

Ethical Deficiency:

- Burleson's lack of ethical standards and disregard for the consequences of his actions on others were critical factors in his decision to commit the crime.

Q.4. What are ethical and legal issues involved with it?

Ans.

Ethical Issues:

- **Breach of Trust:** Burleson violated the trust placed in him as a programmer by using his technical knowledge to harm his employer.
- **Malicious Intent:** The deliberate nature of the attack, driven by revenge, underscores a severe ethical lapse.
- **Impact on Innocent Parties:** The disruption to payroll affected many innocent employees, highlighting the broader ethical implications of his actions.

Legal Issues:

- **Unauthorized Access:** Burleson's actions constituted unauthorized access to the computer system, a violation of computer fraud and abuse laws.
- **Data Destruction:** Deliberately planting a virus to destroy data is a criminal offense under laws protecting digital information and infrastructure.
- **Felony Charges:** The conviction as a third-degree felony with significant penalties reflects the serious nature of the crime.

Q.5. Suggest the way the crime could have been stopped.

Ans.

Technical Measures:

- **Access Controls:** Implement strict access controls to limit the ability of employees to plant malicious software.
- **Monitoring Systems:** Use monitoring and logging tools to detect unusual activities in the system.
- **Regular Audits:** Conduct regular security audits to identify and mitigate potential vulnerabilities.

Organizational Measures:

- **Exit Procedures:** Establish comprehensive exit procedures, including immediate revocation of access privileges for terminated employees.
- **Conflict Resolution:** Develop robust conflict resolution mechanisms to address workplace issues before they escalate.

- **Employee Support Programs:** Provide support programs for employees facing termination, including counseling and career transition assistance.

Educational Measures:

- **Ethics Training:** Offer regular ethics training to emphasize the importance of ethical behavior and the consequences of cybercrimes.
- **Awareness Programs:** Conduct awareness programs about the risks and consequences of insider threats.