Disgruntled Employee Plants Time Bomb in Get-Rich-Quick Scheme

Recently in the US, another hacker went to trial to determine if he will be spending the next several years in jail or as a free man. Unlike many hacker trials, the defendant in this case is not an adolescent, but a 63-year-old systems administrator earning over $160 000 per year with a big-name financial company. After working for the company for many years, the systems administrator came to expect a $25 000 bonus at the end of each year. One year, the company suffered financial losses and the employee received only a $10 000 bonus. The employee had been counting on $25 000 for his son's college tuition. Feeling cheated, the employee began building the code that would punish his employer while creating a windfall for him and his family. According to the prosecution, the systems administrator developed a malicious code to delete files and cause a major disruption on his company's network.

The time bomb was ingenious in design. Working remotely on the corporate system from his home, the employee allegedly built four separate components of the time bomb:

- Component 1, the payload: this destructive portion of the code told the servers to delete files;
- Component 2, distribution: this code pushed the bomb from the central server in the company's data centre out to the 370 branch offices scattered across the country;
- Component 3, persistence: this code kept the bomb running despite reboots and any loss of power;
- Component 4, triggers: to avoid mistakes, he built not one, but two triggers for the bomb. If one trigger was accidentally discovered and deleted from the system, another one would be silently waiting to go off, setting a destructive chain of events into motion.

With the bomb in place, the employee went to his supervisor and demanded the bonus that he felt he was due, and threatened to quit if he didn't get it. Then he packed his things and left. Prosecutors said that "within an hour or so" of walking out the door, he was at a securities office buying 'put' options against his company. 'Put' options are a high-risk, high-payoff type of share trade where the buyer profits if the company stock goes down. Over the three weeks that followed, the employee spent nearly $25,000 to purchase a total of 330 'puts', almost all of them against his company. He had not bought one before that month, and he never bought another one afterward. He purchased more than half of the 'puts' the day before the disaster struck. The damage caused by the malicious code impaired trading at the firm that day, hampering more than 1,000 servers and 17,000 individual workstations. The attack cost the company about $3 million to assess and repair. The prosecution claimed: "It took hundreds of people, thousands of man hours and millions of dollars to correct". The unusual purchase of 'puts' is the primary incriminating evidence against the employee. Investigators also determined that the bomb was planted by someone logged on with the employee's username and password. The employee's primary defence was that other company users could have accessed the system using his password and that the systems were vulnerable to outside attackers. He was jailed for eight years.

Questions

1. Why were the four components of this time bomb considered ingenious?

2. Name the two pieces of evidence you think are most damaging to this employee. Explain why.

3. Based on the information presented here, do you think the employee is guilty beyond a reasonable doubt? Why or why not? Is guilt more difficult to prove in cases of cybercrime as opposed to ordinary crimes?

4. What steps could the company have taken to avoid this type of destruction?

SOURCES: Solheim, Shelley, 'UBS Employee Stands Trial for Detonating "Computer Bomb"', *IDG News Service,* June 8, 2006, www.infoworld.com; Gaudin, Sharon, 'Prosecutors: UBS Sysadmin Believed "He Had Created The Perfect Crime"', *Information Week,* July 10, 2006; 'Disgruntled UBS PaineWebber Employee Charge with Allegedly Unleashing "Logic Bomb" on Company Computers', U.S. Department of Justice (website), www.usdoj.gov/criminal/cybercrime/duronioIndict.