White collar crime and corporate espionage

Law

White-collar crimes have larger repercussions while street crimes have the minute outcome (Green, 2006).

Street crimes give nearly zero percent threat to computer security while white-collar crimes are a major threat to computer security. Street crimes have nothing to do with hacking, stealing computer codes and getting into private and restricted information while white-collar crimes are associated with all these (Green, 2006).

Provide specific examples of both insider and outsider espionage that has taken place over the past 10 years and involved access to digital information. Describe the laws that were broken in each example and discuss the consequences faced by those who perpetrated the crimes. Be sure to include the necessary details of the crime, such as date, location, whether the crime was resolved, etc.

In the year of 2003, a Singapore national was held captive because of his crime of stealing trade secrets in April by the US Attorney’s Office for the Northern District of California. According to his given information, while working for a language translation company, he stole the information and asked for $ 3 million for handing over the information to a competitor (Kabay, 2009).

In the year 2004, an employee of US company’s software Development Center in India, who was herself an Indian national, was held captive in July because of copying the source code of printing identification cards to her

email account (Kabay, 2009).

In the year 2006, two Chinese residents named Fei Ye and Ming Zhong were taken into custody in December because of their stealing information from Microsystems and Transmeta Corporation. There was an arrangement of designing a competitive microprocessor for the city of Hangzhou and the province of Zhejiang (Kabay, 2009).