Computer Crimes and the Criminal Enterprise

Introduction to the Criminal Enterprise

According to the FBI, individuals who join in a definite organization to conduct important criminal activities are known as those who are part of a criminal enterprise (Organized Crime, n.d.). The criminal enterprise, sometimes referred to as organized crime, has very extensive supporting networks magnifying the impact of the criminal enterprise. The criminal enterprise is different from organized crime in that its elements require specific prosecution through statutes. The Racketeer Influenced and Corrupt Organizations (RICO) statute or Title 18, and The Continuing Criminal Enterprise statute, or Title 21 of the United States Code, both define the criminal enterprise as a group of six or more criminals, acting in a management position to generate large amounts of income from criminal activities (Organized Crime, n.d.).

Computer Criminal Threats

A computer criminal threat, as part of a larger criminal enterprise, can operate either within or outside the United States using the computer and telecommunications infrastructure to pose a serious threat to the U.S. government, including most commercial, finance, and defense institutions (Russian Hacker, 2003). The goal of the computer criminal may be for personal or enterprise gain; however, any attack against the U.S. government, including most commercial, finance, and defense institutions, results in loss of market share, proprietary information, funds, reputation and productivity (Russian Hacker, 2003). The computer criminal is also energized through the ineffective use of security computer, network, and telecommunications security controls (Anderson, 1999).

Criminal Enterprise Crimes

Actual computer enterprise crimes use the Internet as the communication backbone to carry out illegal activities such as terrorism, industrial espionage, organized computer fraud, software piracy, credit card fraud, wire fraud, conspiracy, and computer hacking (Computer Crime Research Center, 2005; Russian Hacker, 2003). Unlike in the computer crime in which hackers are conducting operations for personal gain, the actual criminal enterprise crime conducts large-scale computer crimes to provide financial and political support to the overall organization. Other large-scale criminal enterprise operations include identity theft, hacking, child pornography, and embezzlement. The actual use of the computer to conduct criminal activities is considered a felony in violation of section 1030 of the U.S. Code (Types of Computer Crimes, 2005).

Criminal Enterprise Forensic Response

The forensic response to a criminal enterprise operation involves several investigative steps both before, during, and after the criminal enterprise threat has been identified.
The first step in a forensic response is to conduct a review of the alleged computer crime. The investigator will determine the intent and scope of the criminal enterprise investigation, determine resource availability, identify any legal restrictions, and finally determine the facts of the incident (King, 2006). Next, the investigator will review the Preliminary Investigation Discussion information also known as the PID (King, 2006). The investigator would then enter the preservation phase at which time he would photograph and document the crime scene and process the search warrant. Once the search warrant has been issued, the investigator then collects all physical evidence, computer evidence, and digital evidence. Evidence of criminal enterprise activities usually comes in the form of the following:

- e-mail
- graphics
- deleted files
- allocated and unallocated data
- slack space
- swap space on the computer

Lastly, evidence can be found in peripheral storage devices attached to the suspect's computer like cell phones and even PDAs (King, 2006).

**Computer Forensic Outcome**

Once the evidence collection and processing is complete, the evidence providing probable cause to the investigator of the criminal enterprise crime is presented. The investigator must first organize the forensic documentation to ensure all the evidence and the logs are reviewed for disposition of the criminal evidence (King, 2006). Any of the notes collected by the investigator to include expert testimony and witness statement should be audited. Any files related to digital evidence should be archived by the investigator. In addition, all the evidence should be reviewed and audited to ensure all the evidence is present (King, 2006).

After the investigator has audited all the physical and digital evidence, the forensic presentation is developed. The presentation will organize the investigative presentation into a sequence of events known as actions and results (King, 2006). Each event will provide the court with what action was performed, including the reason it was performed and the results of the investigator's actions (King, 2006). After the presentation is prepared, the actual report, identifying the criminal enterprise evidence is prepared revealing only the facts of the case. Once the report is completed, it is archived. It is probable that the evidence will lead to the identification of the criminal enterprise suspects, the initiation of more search warrants against the property of the criminal enterprise, the search and seizure of more evidence, and the prosecution of those maintaining the criminal enterprise (King, 2006).
References


