UC San Diego NEWS RELEASE
University Archives. RSS 6020

Computer abuse seminar for prosecuting attorneys

July 16, 1976

"This computer is so sophisticated that it has defrauded the company without ANY outside help."

--A recent cartoon caption

Computer fraud, perpetrated by operators, accountants, programmers, analysts, and salesmen, is one of the fastest growing white collar crimes in the nation. Currently with some 3 to 7 per cent of the U.S. working force associated with computers in their work, reported computer abuses account for over $200 million in losses annually.

An IBM study estimates that only 15 per cent of the criminal computer abuses are reported and records show that when they are reported, only a fraction of the cases result in prosecutions. Often prosecution depends on the skill of the prosecutor in framing charges as laws based on 19th century definitions do not always apply to 20th century computer crimes.

A week-long computer abuse seminar for prosecuting attorneys sponsored by the University of California, San Diego Computer Center and the U.S. Attorney's office in San Diego will be held July 26-30 at UC San Diego. The first of its kind in the nation for prosecuting attorneys, the seminar is designed to give the attorneys a basic understanding of computer operations, how computer systems are defrauded and a look at patterns of past computer crimes. By obtaining a familiarity with computers, it is hoped that the attorneys will be better prepared to handle computer fraud cases.

"Prosecutors today are faced with various problems when dealing with computer crimes," states David Curnow, chief of the special prosecutions fraud unit in the San Diego U.S. Attorney's office. "One such problem is that the computer criminal is far more sophisticated in computer knowledge," he noted, "which is why this seminar is extremely valuable to our office."

During the seminar, approximately 20 attorneys will use the university's computer system, getting a first-hand knowledge of computer operations. The university's computer center houses IBM, CDC and Burroughs computers that service 120 terminals on the San Diego campus. The program is headed by Edward Coughran, director of the computer center and is funded under a University of California Regents' grant designed to disseminate useful research results into individual campuses' local communities.

"In the press and popular mind, computers are generally given credit for far more ability than they possess," explains Coughran. "There is an easy personification of computers, as though the computer itself could commit a malicious act or be an active collusive participant. But the computer is only a tool, albeit a quite sophisticated one," he added.

The unlawful taking of hardware is easily pinpointed, Coughran says, as it is tangible. But inside a computer, data, or software, is intangible and at times difficult to define. Often computer criminals are insiders in the company and quite skillful, making it easy for them to cover their tracks and their actions hard to detect.

While the abuses are traditional, the mode of perpetration is new and can be best understood from an operational viewpoint. A study at Stanford Research Institute classifies the focus of computer crimes into four categories: input, processing, output and control.

Input, or the entry of data into a system, can be falsified or altered on otherwise authentic programs. A Canadian incident involved an employee who altered the account number and address of deceased pensioners to his own account and thereby collected their pension payments. Processing involves the manipulation of information within the computer, including the transferring of accounts or masking of information. One case involved a programmer who put a program "patch" into a bank system to cause it to ignore overdrafts on his account.

Output, the printed material from a computer, can be altered as was the case when an employee hit the repeat button on a printer and caused multiple copies of his legitimately prepared paycheck to be produced. Control, or the ability to affect the total computer system, is used by individuals in supervisorial positions. The Union Dime Savings embezzlement case is a good example of control computer crime. A head teller transferred money between accounts, depending on when the interest was to be calculated, and eventually netted $1.5 million.

"Undue reliance on a computer report and failure to look behind it to the truth or existence of the data it purports to reflect, may subject the overly credulous to liabilities," Coughran says. "The acceptance of the computer as irrefutable and the disbelief that data processing personnel would even consider criminal action, contributes to the high rate of computer crime."

Coughran says that there is an inherent faith in computers and that to most, computer printouts are authoritative.

"For instance," he points out, "if your bank statement is different than your ledger, the first thing you will do is check your addition."

He warns against complete reliance on computer reports, noting, "computers can be programed to lie or conceal as easily as they can be programmed for the truth."

(July 16, 1976)