Cybertrust "How the Heck Did This Happen" Presentation
Case B - 1
Full story available at:
http://cbs5.com/localwire/localfsnews/bcn/2006/01/20/n/HeadlineNews/INDICTMENT-MEDICAL/resources_bcn_html
March 2005

SUSPECT IN SJ MEDICAL DATA THEFT TO BE IN COURT MONDAY

A federal grand jury has indicted a former San Jose Medical Group employee for stealing computer equipment from the health care provider, including a digital video disc containing medical records for approximately 200,000 group patients.

Joseph Nathaniel Harris, 43, is currently free on $25,000 bail. He was arrested on Jan. 3. If convicted he faces a possible 10-year prison sentence.

According to federal prosecutors, Harris, a branch manager for the medical group, was asked to resign in the fall of 2004. The following March, group employees discovered computer equipment was missing from the organization's main office, including the DVD. The FBI began an investigation and allegedly discovered the DVD in Harris's car. Harris is scheduled to return to U.S. District Court in San Jose on Monday.

Cybertrust "How the Heck Did This Happen" Presentation
Case B - 2
Full story available at:
http://news.com.com/Medical+group+Data+on+185,000+people+was+stolen/2100-7349_3-5660514.html
March 2005

A California medical group is telling nearly 185,000 current and former patients that their financial and medical records may have been exposed following the theft of computers containing personal data.

Given the number of people affected, the theft from the San Jose Medical Group ranks among the largest in the nation. It follows a rash of other breaches that have raised concerns about the security of sensitive information.

The theft occurred after the San Jose Medical Group had copied patient and financial information from its secured servers to two local PCs, said Mike Patel, vice president of information technology for the San Jose Medical Group.

The data, some of which was encrypted, was part of a patient billing project and also part of the medical group's 2004 year-end audit, Patel noted.

On March 28, during the early morning hours, the building was broken into and the medical group's two new Dell computers were stolen.

"We believe they were stolen because of the kind of computers they were and not because of the information," Patel said, noting that there have been no reports of patients' personal or financial information having been compromised.

Ironically, the medical group earlier this year began the process of encrypting its patient and financial information. It had not completed the process when the two PCs were stolen.

"We started to encrypt things this year because of (medical regulations), ID theft reports and security regulations," Patel said.

As a security measure, the medical group has historically stored its information only on the secured servers, where employees have only limited access to the computers and the information can only be accessed via the network.

Under the Security Breach Information Act of California, companies and organizations are required to notify people when their personal information may have been stolen. The San Jose Medical Group began notifying patients on Tuesday, nine days after the break-in, Patel said. He noted that it took some time to gather the necessary information for notices and then distribute them to the thousands of patients who were affected.

Since the burglary, the medical group has taken steps to shore up the physical security of the building with surveillance cameras and other measures, Patel said.

Cybertrust "How the Heck Did This Happen" Presentation
Case B - 3
Full story available at: http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/05/15/THEFT.TMP
March 2005

Arrest in theft of records
South Bay patients' medical data stolen

A former branch manager at a San Jose medical group has been charged with stealing the confidential records of nearly 185,000 patients -- mostly South Bay residents, authorities reported.

The San Jose incident is one of the nation's largest cases of personal data theft, even bigger than the highly publicized case of ChoicePoint, in which the personal information of 145,000 people was sold to an identity theft ring posing as a legitimate business in September 2004.

The U.S. attorney's office charged Joseph Nathaniel Harris on Friday with stealing two computers and a compact disc that contained patient records from the San Jose Medical Group on March 28, according to a complaint filed in U.S. District Court in San Jose.

The FBI reported in court documents that the disc with patient information was recovered after Harris' arrest. In an interview with FBI agents, Harris said he didn't know the patient information was contained on the stolen CD until he saw media accounts of the theft, according to court records.

Harris made contradictory statements on how he came into possession of the data, according to court records. "I'm not sure how I got this CD," Harris was quoted as saying. "I think we probably know how I got it."

Harris, who is being held without bail, could not be reached for comment Saturday and it is unclear from court records filed Friday if he has an attorney.

After the burglary, San Jose Medical Group CEO Ernie Wallerstein in April notified at least 185,000 patients that their data was compromised. The missing disc contained a wealth of patient data, including names, addresses, Social Security numbers, dates of birth, insurance data, bill records and detailed medical histories.

According to court records, Harris is suspected of selling the stolen computer equipment on the Internet through Craigslist just after the medical office burglary. He is also suspected of burglarizing his brother's home in Scott's Valley in December after Harris was videotaped purchasing items with an allegedly stolen credit card, court records state.

Harris worked as the branch manager of the San Jose Medical Group's McKee clinic at 227 Jackson Ave. in August and September of last year, court records said. "During Harris' employment at San Jose Medical Group, there were several incidents of reported theft of money and medications," according to an affidavit by FBI Agent Deborah Amrhein. "Because of these suspicions, Wallerstein asked Harris to resign. ... Harris complied."

During his employment there, Harris "bragged to fellow employees of his experience as a Green Beret, in military security and about his side business selling used computers," Amrhein wrote in the affidavit. After he resigned, there were six burglaries at three San Jose Medical Group offices.

Amrhein also reported that Harris had been fired from a 2003 job at the Silicon Valley Children's Fund for conducting personal business, including selling computers on Craigslist, on company time. After he was fired from that job, there was a burglary at the Children's Fund offices and two computers were stolen.

On April 15, Harris canceled a voluntary interview with federal agents, saying he was in Coalinga (Fresno County). But a day later, he was arrested by local police in Campbell on suspicion of auto theft. During a jailhouse interview with Amrhein, Harris allegedly admitted selling stolen computers and offered to lead police to the missing disc if released. Agents later found the disc in Harris' Hyundai Santa Fe.