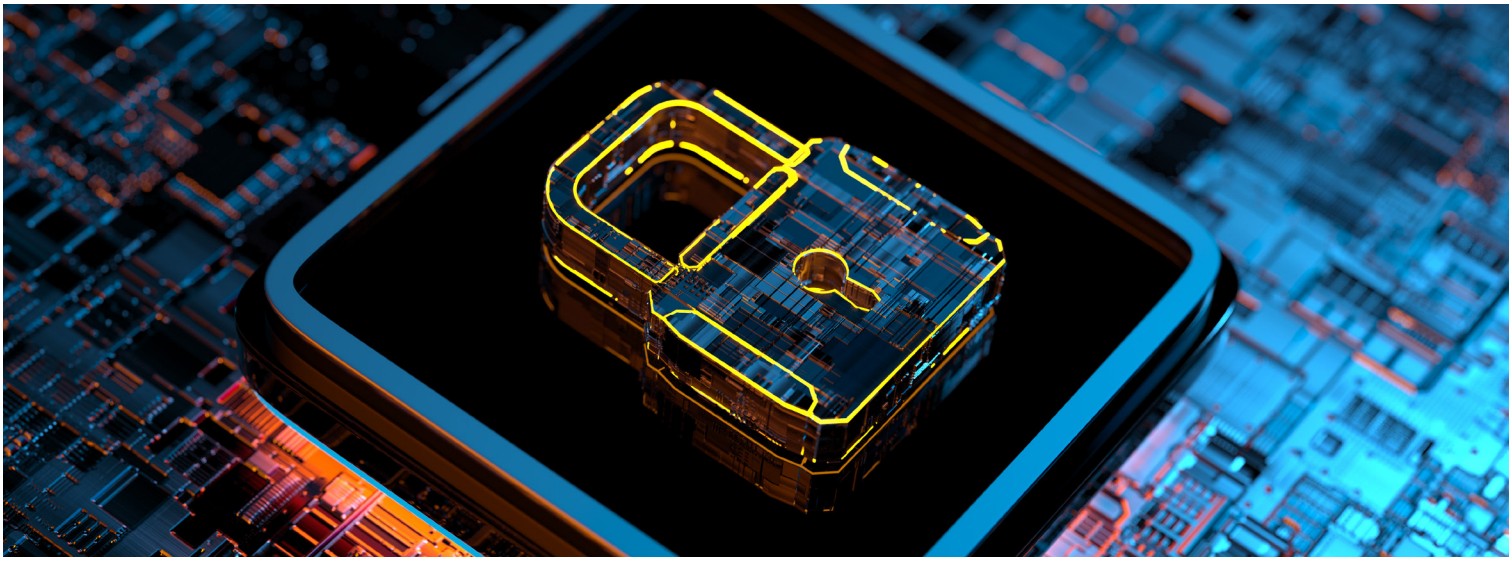

Nervous System: Dumpster Diving for Fraud and Profit

BY DAVID KALAT

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have been with us longer than we remember.

Nervous System *is a monthly series that approaches issues of data privacy and cyber security from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*

Jerry Schneider was a clever man who had an art for the hustle. As a high school student in 1968, he launched his own startup, selling electronic communication devices he invented using parts he scavenged from the dumpsters of Pacific Telephone and Telegraph (PTT). Taking advantage of his superior knowledge of PTT's inventory tracking systems, Schneider found he could skip the need to refurbish scrap from their trash and instead resell them their own existing inventory at a pure profit to himself. His case became a landmark study in early computer crime, even though he did not use a computer himself to commit the crime. Instead, Schneider exploited his knowledge of the victim's computer systems to cover his tracks.

As a teenager, the precocious and intrepid young man ran his own company, Creative Systems Company, selling wholesale electronics parts and his own electrical inventions. Much of Schneider's business came from selling refurbished equipment from the Western Electric Company, a wholly owned subsidiary of AT&T that provided equipment to the telephone companies.

On his route to and from high school, Schneider passed PTT—specifically, their dumpster. It behooved him to harvest what he could from Pacific Telephone's trash to adapt, recycle, and refurbish parts. In some instances, PTT had junked perfectly new equipment from Western Electric still sealed in its original packaging.

The telephone company also discarded extensive documentation and instruction manuals. Over time, Schneider reconstituted a nearly complete library of PTT's operational documentation, including detailed explanations of the company's policies and procedures regarding inventory management.

Posing as a journalist, Schneider received a thorough tour of Pacific Telephone's facilities, complete with special presentations on the process of ordering supplies. He was given copies of key documents and introduced to top decision makers. By the summer of 1971, Schneider was reasonably sure he knew more about PTT and Western Electric's internal operations than any of their employees.

Schneider obtained one of Pacific Telephone's service vans simply by buying it from them at an auction. It still had the company's emblems emblazoned on the body work. He obtained a key to one facility from a disgruntled employee and used the access to duplicate keys for other sites. He posed as an employee and obtained computer login codes by asking for them.

Once the groundwork had been laid, the fraud itself was simple. Schneider would place an order for telephone and computer equipment from Western Electric, masquerading as Pacific Telephone. Then, he knew exactly when to present himself at the victim site when the delivery was made, fill out the necessary paperwork, and load the equipment into in his seemingly legitimate Pacific van.

Key to the scam was Schneider's superior understanding of PTT and Western Electric's billing systems. He knew how much Pacific Telephone had budgeted for equipment purchases each quarter, and how much they typically ordered. As long as his fake orders fit into the difference between what PTT actually spent and they were willing to spend, no one would scrutinize the invoices closely enough to spot the discrepancy.

In fact, most of Schneider's business as Creative Systems Company was legitimate. He genuinely refurbished used equipment and resold it, more often than not. But somewhere around forty percent of his sales came from the equipment he obtained through fraud.

As time went on, he discovered he could order equipment from Western Electric to be delivered to unsecured industrial sites where he could retrieve it without as much personal risk of exposure. Another clever trick was to "buy" enough volume of certain types of equipment to drive down the inventory levels to the point where he knew Pacific Telephone would be compelled to buy more, and then resell the stolen equipment back to them to bring their inventory back up.

Schneider kept his scam going for seven months. He likely could have continued it much longer if he had not confided his secret in one of his employees. That person tried to blackmail Schneider for a better salary, and when Schneider refused, the employee called Pacific Telephone.

When Schneider was arrested, it was unclear exactly how much he had stolen. Prosecutors decided he had taken $125,000 in all, but Pacific Telephone, mindful of the public relations problem, insisted it was no more than $65,000. Computer criminologist Donn Parker wrote extensively about the case and estimated the actual theft was more likely in the millions. Schneider ended up pleading guilty to grand theft of $5,000 (the value of the specific equipment in his possession at the time of arrest). He paid a $500 fine and spent forty days in jail.

After serving his time, Schneider started a new business, Security Analysts (later EDP Security). As a computer security consultant, he advised clients how to keep people like him for doing the things he had done. He offered his services to Pacific Telephone. They declined.

Legaltech® news

This article was originally published in Legaltech News on September 1, 2021.