FEBRUARY 5, 2018

Legaltech® news

ONLINE

An ALM Publication

Nervous System: The Story of the First White Hat Hacker

'Nervous System,' which approaches issues of data privacy and cybersecurity from the context of history, kicks off with a look at Milo Arthur Bennett's 1960s computer escapades.

BY DAVID KALAT

With the aggressive pace of technological change and the seeming onslaught of news regarding data breaches, cyberattacks, and technological threats to privacy and security, it is easy to mistakenly assume these are fundamentally new threats. In fact, the pace of technological change is perhaps slower than it feels, and many of these seemingly new categories of threats have been with us longer than we remember. "Nervous System" is a bimonthly blog that approaches issues of data privacy and cybersecurity from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.

As a professional computer examiner and a testifier on computer forensics, I wanted to understand better the history of my own profession. To that end I set out to research the *earliest* computer forensic case I could identify. That research led to my article "Day One: The Origin Story of Computer Forensics," published in the debut issue of *Pratt's Privacy & Cybersecurity Law Report*.

I chose the story of Hugh Jeffery Ward and his 1971 prosecution for theft of trade secrets because that case involved the engagement of a computer professional to preserve and examine electronic data, and to opine on those findings at trial. During my research, I discovered computer fraud and abuse cases from as long ago as the 1950s and 1960s that did not qualify as the first "computer forensic" examination, because their investigations did not depend on the collection and examination of electronic evidence. Nevertheless, these cases involved electronic crimes, and I would like to share one story.

The earliest-ever media report of a computer crime was published on October 18, 1966, with the *Minneapolis Tribune*'s front-page headline "Computer Expert Accused of Fixing His Bank Balance." This led to what may be the first instance of what we would now call a "white hat hacker."

According to the *Tribune* story, in 1965 the National City Bank of Minneapolis had implemented a computer

system to manage checking accounts. Milo Arthur Bennett was a programmer working for the contractor hired to install and manage the new system, called NCB Program 107. In the framework of the classic "fraud triangle," occupational fraud arises when there is 1) a perceived opportunity 2) to resolve a perceived secret financial problem, and 3) a rationalization to make the fraud psychologically acceptable.

Bennett had all three legs of that particular stool. As one of the few specialists with access to the inner workings of the new computer system, he had a level of opportunity to manipulate its operation. He also had a financial problem, owing $334 more than he had in the bank (Bennett was also a banking customer at National City). He had a rationalization, too—telling himself that he only needed to temporarily "float" himself some funds and would replace the money before anyone noticed it was missing.

According to the media coverage and subsequent court filings, Bennett wrote some extra code, patching the software so that in its exception reporting it would simply ignore overdrafts on his personal account. Anyone looking at the actual daily balances would have seen the overdraft, but the bank apparently relied on the exception reports rather than perform individual monitoring of each account.

Regardless of whether Bennett ever intended to replace his overdrawn balances or this was merely a happy lie he told himself, by September 1966 his overdrafts had accumulated to $1,357—the equivalent of over $10,000 today. Finally, a computer failure forced the bank to temporarily switch back to manual processing, at which point the discrepancy in his account was discovered.

The FBI investigated, and the 23-year-old programmer confessed. He reportedly made restitution to the bank, and in exchange received a suspended sentence. His prosecution in January 1967 is reported as the first-ever federal case involving the criminal use of a computer.

Meanwhile, a technologist by the name of Donn B. Parker was working on drafting guidelines for professional conduct for the Association of Computer Machinery. He had become increasingly concerned by the risks that new computer technology could be used for fraud or other criminal activity, but had struggled to get others in his profession to focus on those risks. When Parker read the article in the *Minneapolis Tribune*, he sought the participants to conduct his own investigation and to interview Bennett directly. Parker wrote a report on the incident, using it as a keystone to indicate the need for ethical standards in computer usage.

That led Parker to research other computer crimes, funded in part by the Stanford Research Institute and published in such books as *Crime by Computer* (1976). Parker also began publicizing the need for improved cybersecurity (a term not in use at the time, but it is how we would classify his work today). In 1971, Parker reported he was engaged by various institutions to actually attempt to embezzle from them using electronic methods in order to identify data security vulnerabilities. He entered into a special arrangement with a London bank to receive his "ill-gotten" gains from his various successful hacks and frauds, from which the monies would be repaid to the victim institutions along with an explanation of how he had taken them.

As quoted in Gerald McKnight's 1973 *Computer Crime,* Parker said, "They—the firms I'm embezzling from—indemnify me. I go to them in the first place and tell them I can break their security. If they doubt it, I offer to prove it to them. If they want to know how good their security is, the lesson is bound to be to their advantage."

Parker's passion for the issue was striking, and today's cybersecurity and information privacy professionals owe him a tremendous debt.

David Kalat *is Director, Global Investigations + Strategic Intelligence at Berkeley Research Group. David is a computer forensic investigator and e-discovery project manager. Disclaimer for commentary: The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.*