Case 4

"Ethical Hacking"

Randal Schwartz worked for Intel Corporation from 1988 to 1993. While working in the iWarp division (later incorporated into Supercomputer System Division (SSD)), he recommended that they institute some fairly basic security practices, such as using strong (hard-to-crack) passwords. In 1991, he began running a password-cracking program called "Crack" on the password list for the division to insure that all users' passwords were strong. He left that division in 1992 and moved to another division within Intel. In 1993, while a system administrator in his new division, he became concerned that the security might have become lax since he had left SSD. A security breach in one division easily compromises every machine in the network. Using an old account in SSD, he downloaded the password file from the cluster of computers in SSD and ran Crack on it, breaking 48 weak passwords, one of them that of a vice president. This was a serious weakness.

Unfortunately for Schwartz, another employee noticed the activity, and reported it before Schwartz had a chance to inform Intel of his findings. Intel contacted the police, and he was subsequently tried under Oregon State law ORS 164.377, and convicted on three counts of computer crime. The law reads, in part, "Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime." This crime is a Class A misdemeanor. Furthermore, the law labels as a Class C felony the act of altering, damaging, or destroying any computer, computer system, or computer network if the act is done knowingly and without authorization.

As a convicted felon, Schwartz lost the right to vote, to serve in a public office, or to serve on a jury. In 2007, however, Schwartz's record was expunged. The court order read, in part, "The defendant, for all purposes of the law, shall be deemed not to have been previously convicted or arrested."

Recently, a few schools have been offering certification programs in "ethical hacking," that is, the art of hacking into computer systems for good purposes. UMBC Training Centers, in Maryland, offer a non-credit program, called "Certified Ethical Hacker," that promises to prepare students for taking the EC-Council (International Council of E-Commerce Consultants) Certified Ethical Hacker exam 312-50. According to the EC-Council's website, an ethical hacker is "an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a hacker." The website warns that hacking is a crime in the United States and in many other countries, but points out that it is legal "when it is done by request and under a contract between an Ethical Hacker and an organization."

Such programs are also offered in other countries. Tilak Maharashtra University offers a three-semester long Advanced Degree in Cyber Security. Sunny Vaghela, a prominent ethical hacker in India, hosted a workshop at the Tryst science and technology festival, put on annually by the Indian Institute of Technology Delhi. As reported in a May 16, 2010 article in the Economic Times, Vaghela said, "At the workshop I highlighted some of the common yet neglected cyber crimes. I hacked into major government and private websites and later issued an advisory to these, suggesting possible solutions.''