TruSecure Corporation
"Planning for Failure" Presentation
Case B
Full story available at USAToday.com/moretech
4/7/2003

Tiny Nevada hospital attacked by Russian hacker

RENO (AP) — A hacker who invaded the computer system at [Case C] hospital in Ely has been traced to the former Soviet Union, authorities said. The FBI said the hacker used the Web site of Al-Jazeera, the Arab news network, as a conduit to the hospital.

Officials at the 40-bed hospital said patient records are safe, but added that the cyber intruder may have accessed employee Social Security and bank information.

The incident has resulted in improved computer security at Nevada's other rural hospitals and serves as a lesson for all computer users.

"Here's tiny Ely, a place where people leave doors unlocked, and we get hacked by the Russian Mafia, who are pretending to be Arab terrorists, because they are the people to blame this week," Jim C., information technology manager for the Ely hospital, told the *Reno Gazette-Journal.* "We may be remote in geography, the most distant city from any metropolitan area, but with the Internet we might as well be in downtown New York or Los Angeles."

Jim C. detected the Ely break-in on March 20. "It was just after 6 a.m. and I saw an active connection from outside, on a path through the emergency room to the payroll computer, but I knew no one was in the payroll office." He said he ran to the affected computer and pulled the plug.

Jim C. said the system seemed to be protected from attacks. But the FBI lab's analysis of the hospital's hard drives showed a game program, *Blaster Ball,* contained a Trojan horse, a hidden code that acted as a beacon and let hackers into the hospital's system.

"Two employees admitted downloading the game from the Internet and installing it at a work station," Crosley said. "The Trojan horse reported back to the hackers, and the system was compromised. It was an eye-opener that you can have the best firewall available, but someone on the inside can unintentionally blow it out."

Bob M., hospital administrator, said the intrusion resulted in tighter policies and procedures, and more security measures.

"Payroll is off the network," he said. "We've told employees never to install software or sign on to streaming Internet services."

Jim C. said the Ely hospital's security measures routinely fight off between 40 and 60 electronic attacks a day. Computer experts said all Internet connections are vulnerable to electronic vandals, whose motives range from bragging rights to identity theft.

"Ely isn't remote any more," he said. "On the Internet, the world and all the bad guys in it are as close as your desktop PC."