

Cyberattacks against critical U.S. networks rising at a faster rate

By Jill R. Aitoro 12/08/09

The number of cybersecurity attacks against computer networks that operate the nation's critical infrastructure such as transportation systems and water treatment and power plants, has increased dramatically, mostly because these industries rely on legacy technologies that don't protect systems from sophisticated attacks.

In the third quarter, 11 cyber incidents were added to the Repository for Industrial Security Incidents, a database of cybersecurity attacks that have or could have affected systems that operate major industrial operations in the United States. These key networks are known as Supervisory Control and Data Acquisition systems. The owners and operators of industrial plants maintain the database.

For all of 2009, industries have added 35 incidents to RISI, representing more than 20 percent of the 164 incidents recorded since 1982. The total number of incidents in the database could increase 37 percent this year if trends continue at the current rate, according to [RISI's third-quarter report](#), which was released on Nov. 30.

Malicious software such as viruses, worms and Trojans were the cause of most cyberattacks, according to the report. Incidents involving unauthorized access or sabotage by people working for the company such as disgruntled former employees or contractors also increased.

"Unfortunately, it's all hitting the fan," said Jake Brodsky, control systems engineer with the Washington Suburban Sanitary Commission, at the SCADA and Control Systems Security Summit in Vienna, Va., on Tuesday. "We have operations to concern ourselves with, public safety. And at the same time, we have to be aware of the latest and greatest technology and any [associated] security vulnerabilities. We're trying to merge all of this together and come up with a system that just plain works."

Old technology presents a particularly difficult problem to solve. While most computer systems are upgraded every three to five years, control systems typically remain operational for up to 20 years, said Sean Paul McGurk, director of control systems security at the Homeland Security Department. These old systems were not developed to function in a networked environment or combat the onslaught of cyberattacks.

"The introduction of [commercial] technology into the [SCADA] environment means that we migrate into these industrial networks" the same vulnerabilities that exist in traditional information technology environments, he said. "We'll buy blade servers, stick them in a process-network environment, and not understand how to configure them for an industrial control environment."

McGurk said network managers are concerned about zero-day vulnerabilities, which are exploited before the vendor has a chance to create patch, but for control systems, "you're worried about zero-decade vulnerabilities."

Government officials, working with executives from companies operating critical infrastructures and the vendors that support them, are developing security standards through the DHS [Control Systems Security Program](#). Homeland Security also established the Critical Infrastructure Partnership Advisory Council to ensure that those individuals and companies with a stake in protecting major systems contribute to policy decisions.

"We're bringing individuals to the table for the purposes of arriving at consensus," McGurk said. "We get the like minds that

understand the challenge together with the policy wonks and regulators figuring out how to make [cybersecurity standards] real and actionable on the plant floor. Government does not have all the answers. By and large this problem is going to be solved by the private sector."