

[See full article and related items](#) | [Print](#)



FBI Reaches Out to SCADA Users

September 2nd, 2008

Written by Wes Iversen, Managing Editor

If a cyber security incident occurs at your plant, the Federal Bureau of Investigation would like to hear from you.

If a serious cyber security incident occurred in your plant, would you call in the FBI to investigate?

The Bureau certainly hopes that you would. To encourage such actions, the FBI is taking steps not only to strengthen its agents' understanding of control system technology, but also to build stronger bridges to the control systems community.

The Federal Bureau of Investigation, or FBI, already has trained cyber investigators in all of its 56 field offices, said Scot Huntsberry, supervisory special agent, FBI Cyber Division/Computer Intrusion. Now, the Bureau is looking to identify and train a group of agents to respond specifically to cyber security incidents involving supervisory control and data acquisition (SCADA) systems, he said.

Huntsberry made his comments during a law enforcement perspective panel on control system cyber incident handling at the Process Control Systems Industry Conference, Aug. 26-28 in La Jolla, Calif. "Within the SCADA program, we're looking for outreach opportunities, such as this conference, to initiate relationships with folks in the [control systems] community, so that you know who to call within your specific areas when a cyber intrusion occurs," Huntsberry told the audience.

Disappearing servers

Both Huntsberry and Jeff Morgan, a Process Control Systems Analyst in the FBI Cyber Division, conceded that the Bureau may not have the best reputation in the control systems community for some of its past cyber investigation techniques. In some cases, for example, hard drives or servers may have been removed and taken to an FBI lab for evidence gathering, without apparent regard for system downtime at the company that was victimized by a cyber intrusion.

But the FBI is now making an effort to change its cyber investigation approach to be more cognizant of industry needs and concerns. "We are trying to tailor our response to be sensitive to your competitive interests to get up and running again, and at the same time minimize our footprint at your facility that turns into downtime," said Morgan.

The same is true in Canada, where the Royal Canadian Mounted Police (RCMP) are taking a similar approach. "Law enforcement evidence gathering procedures don't have to conflict with process control system uptime," said Clint Baker, a sergeant in the RCMP's Integrated Technological Crime Unit, who also participated in the panel session.

Information protection

Another inhibitor to calling in Federal agents is the fear that critical information obtained by investigators might be accessible to the media and others. But the United States and Canada both have laws on the books that protect sensitive “critical infrastructure” information, said panel participants. In the United States, the Department of Homeland Security’s Protected Critical Infrastructure Information program protects qualified information from disclosure under the Freedom of Information Act, state and local disclosure laws, or for use in civil litigation.

FBI panel participants urged conference attendees to check their companies’ disaster recovery plans to be sure that if a cyber incident occurs, that law enforcement contact is included somewhere within the plan.

Even when it is unclear whether a crime has been committed, control system users should “error on the side of calling” the FBI, said Huntsberry. “I think that if you do make that telephone call, you will be pleasantly surprised by the fact that someone on the other end of the line is interested, and will probably, within the next couple of hours, be at your facility asking more questions, asking how they can help, and helping you understand the extent of the problem,” he observed.

Among other things, U.S. industrial control system users might look into joining the InfraGard National Members Alliance—an organization with 26,000 members that focuses on information sharing between the private sector and the FBI, as well as other law enforcement agencies.

Call today

As a way to build the contacts now that may be needed later for a quick and effective FBI response to a cyber intrusion, Huntsberry suggested calling your local FBI field office today. “Ask to speak to the cyber squad,” he advised. “Tell them who you are and that you would like to have an agent come and visit, so that they have an awareness of what your facility does and what potentially could be a problem at your site, and to build a working relationship so that you know who to call if needed, so that we can make that quick response happen.”

Federal Bureau of Investigation

www.fbi.gov

Royal Canadian Mounted Police

www.rcmp-grc.gc.ca

Print