

U.S. gets new cyberterrorism security center

Its goal is to better protect critical private industries

News Story by [Todd R. Weiss](#)

APRIL 21, 2005 ([COMPUTERWORLD](#)) -

PHILADELPHIA -- A new private-sector cyberterrorism security center that aims to watch over much of the nation's critical business infrastructure with its own real-time cyberthreat-detection network opened here today at the University of Pennsylvania.

The [Cyber Incident Detection Data Analysis Center](#) (CIDDAC) was unveiled as a real-time defense against cybercrime and cyberterrorism for key businesses in the U.S. that could be targeted by terrorists.

Charles "Buck" Fleming, executive director of CIDDAC, said the organization is believed to be the first private, nonprofit group to set up a cybercrime-detection network outside of the government's own efforts to watch over critical business operations. The group's concern, he said, is that without constant monitoring, critical U.S. industries such as banking, transportation, energy, 911 services and water supply systems could be disrupted by terrorists or criminals -- with disastrous results for the country and the U.S. economy.

While government agencies such as the FBI and the Department of Homeland Security already get reports of cybercrime and cyberterrorism, the agencies aren't always able to respond to threats immediately because of red tape. And companies that are victims aren't always happy to share their information with the government, Fleming said.

"Eighty-five percent of all the [nation's] data is in the private sector, so we realized this has to be a private sector operation," he said. "Companies don't want the FBI looking at their information, even if they're not doing something wrong."

Fleming added, "We realized that coming down the road there are major potential problems that are not being addressed right now."

Under a pilot project, CIDDAC is offering its intrusion-detection services to critical industries using specially built Remote Cyber Attack Detection Sensor (RCADS) appliances that will be installed by the group outside of a business' corporate network, he said. The RCADS will be able to instantaneously and automatically report any attacks to the CIDDAC center, where the intrusion data can immediately be evaluated and quickly passed on to law enforcement agencies. The sensors are not connected to any actual corporate production systems but appear to intruders as just another machine on the network.

Law enforcement officials will be able to use the intrusion data to compile attack signatures, which provide government investigators with data so they can more quickly identify, locate and neutralize cyberthreats,

according to the group.

John Chesson, a special agent at the FBI in Philadelphia, said the RCADS are essentially "hardened honeypots" that look like they are part of the network an intruder is trying to enter. When the RCADS are attacked, CIDDAC workers monitor the event and collect real-time data that can be forwarded to law enforcement officials, he said.

Shawn Henry, an assistant special agent at the FBI, said the CIDDAC initiative "will have national implications." The FBI and other law enforcement agencies will be able to use the intrusion data collected to prevent future attacks rather than just react to incidents, he said. "The commitment that CIDDAC will have from us ... is to continue to track down these cybercriminals."

Brian Schaeffer, a member of CIDDAC's board and the chief technology officer at Liberty Bell Bank in Cherry Hill, N.J., said he thinks that the new program adds an important weapon for defending systems against attacks.

Schaeffer said intrusion data is currently collected on a company-by-company basis, making it less useful in cases of large-scale attacks. "If I can get some intelligence on another financial institution and how they are being attacked and what they are doing to defend themselves, that's more likely to help me," he said.

The initial 30 participants, who are anonymous for security reasons, will pay about \$10,000 for the installation of the RCADS and for the first year of monitoring and reports.

"We take minutes to analyze what now takes hours," Fleming said. "We know it's going to work. We've had prototypes working for years now."

For businesses that use the service, a key benefit is better protection without the need to give up corporate data to government or law enforcement agencies, Fleming said. "Privacy, trust and anonymity are absolute essentials for the private sector to participate, and without the private sector, there is no program."

CIDDAC expects to gain more members and grow into a critical mass that in six to eight months will allow it to effectively monitor much of the nation's business infrastructure, Fleming said.

The pilot project, which has been in the planning stages for two years, is being funded through a \$200,000 grant from the DHS Science and Technology Directorate and with the support of the FBI, according to the group. The center is located in the University of Pennsylvania's Institute of Threat Analysis and Response (ISTAR) laboratory, which has been designated as the home of the CIDDAC National Operations Center. The center is expected to be in full operation by the end of the year.

Harvey Rubin, a professor at the University of Pennsylvania School of Medicine and director of ISTAR, said it's fitting that the project is being done on the same campus where 60 years ago the first large-scale computer, ENIAC, was built. Working to detect and prevent cybercrime is a key issue for the nation, he said.

"It's one of the most serious problems we face in terms of security and strategy," Rubin said. "We fully anticipate that this pilot project will just explode into a large and important enterprise."

CIDDAC evolved from the Philadelphia chapter of [InfraGard](#), an FBI-sponsored information-sharing and analysis program that involves the FBI, the National Infrastructure Protection Center, businesses, academic institutions, and state and local law-enforcement agencies.