

S.A. examining its cyberdefense

By Ron Wilson

San Antonio Express-News

Web Posted : 09/10/2002 12:00 AM

If terrorists launched an attack against San Antonio's computer networks, how would local authorities communicate with federal agencies to exchange information?

Flash graphic

- [Three-phrase disaster drill](#)

To view the graphic you must have the [Flash plugin](#).

Or if a hacker shut down the electric power grid, who should be notified and how?

Those are some of the questions government and business leaders will tackle Friday during Operation Dark Screen, the first phase in a three-part disaster drill dealing with defense against a cyberassault.

Participants hope the exercise will become a model for other cities' disaster plans, said Greg White, a professor at UTSA's Center for Infrastructure Assurance and Security, who is planning the drill.

"This will be a tabletop exercise," or a brainstorming session, he said.

About 100 people will take part, said Assistant Fire Chief Mike Miller, head of the city's emergency efforts.

During Dark Screen, participants will break into groups of eight to 10 people. Each group will get a "what if" scenario and will determine what to do, whom to call, and how to establish communications, Miller said.

"One scenario we'll look at is what to do if someone shuts down the power grid," Miller said.

Or if there's an attack on the financial system, he said, "we need to know how to respond, because we're all involved."

Both White and Miller said an attack doesn't have to be caused by terrorists, but could come from anyone with a grudge against the city.

The exercise is important, Miller said, because hacking, or launching attacks against computer systems — "even your home computer" — has become so common.

Leaders will figure out what agencies they'd need to link up with, and how they'd do it if the city's computers couldn't communicate with each other, he said.

Though other cities have run drills before, this is the first time a computer attack will be studied in depth, with an eye toward creating a model other cities can use, White said.

Dark Screen was born out of a suggestion by U.S. Rep. Ciro Rodriguez, White added.

Because of the terrorist angle in a possible attack, one important participant in Dark Screen will be the supersecret Air Intelligence Agency, White said.

The AIA will look at what type of information, if any, it could share with local authorities, and how that information could be shared securely.

Dark Screen will seek holes in local computer defenses.

Sensitive information gleaned from the exercise will not be made public.

"We're not interested in providing roadmaps to folks hostile to the city of San Antonio," White said.

Phase II will begin Monday. Planners will look at the security holes and decide how to plug them.

In the spring, possibly in May, Phase III will take place. That's when someone will launch a "white hat," or authorized attack on the city's computer infrastructure.

Though Phase III sounds simple, it's almost a nightmare in logistics, White said, because of all the legal permissions that must be in place before the attack can be launched.

rvwilson@express-news.net

09/10/2002

[Click here to return](#)