Business Review
Western Michigan

PIVOTGROUP
Armed with Information Security Knowledge

E-security risks keep security chief up at night

By Lynn Stevens
lynns@mbusinessreview.com

Keeping business information safe in a dangerous cyber world requires a change in corporate culture, according to Dan Lohrmann, Michigan's first chief information security officer and director of the state's Office of Enterprise Security.

Lohrmann

"When you think about security, it's not just I.T.'s job. It's how you interact with information at your company, and are you being cyber smart?" Lohrmann said. "In all of our businesses, wherever you're at, security has got to be part of the culture we live in."

Lohrmann will be the keynote speaker at glimaSouthwest's Tech Expo 2007 Oct. 4 at **Western Michigan University**'s Fetzer Center.

Michigan has won national awards for its e-security, and Lohrmann will share strategies for businesses at the free public expo. He especially encouraged CFOs, their staffs, auditors, directors and managers to attend to find out what risks lurk in cyberspace.

> "People don't realize a lot of old equipment can't be protected because it's not being supported (by the manufacturer) anymore."
>
> **Dan Lohrmann**
> State's chief information security officer

"Cyber crime is growing at an enormous rate," Lohrmann said. "You're just seeing an explosion in cyber crime."

It's organized crime and it's worldwide, he said. It's one of the e-security risks that wakes him at night.

Faith Heikkila, Kalamazoo-based Great Lakes regional security services manager for **Pivot Group**, agreed the hacker game has turned professional. And the hackers may be paid by crime bosses in foreign countries — some advertise for hacker services on the Web, she said.

"It used to be, the 16-year-old kid playing around with a computer was the one you had to worry about," Heikkila said. "Now it's organized crime and some of the foreign-espionage players."

Portable media devices of all kinds are vulnerable, she said. Hand-held devices are easily misplaced or stolen. Most of them cannot be encrypted, according to data Heikkila cited in her recent article for *IEEE Security & Privacy*, an international electronics journal. Data is easily siphoned from them. There is even a program, slurp.exe, which Heikkila said can download more than 20,000 files in a hour into an iPod.

And portable devices used with business computers become recognized objects that can bypass intrusion-detection systems and antivirus safeguards, she wrote. If they don't already have them, companies need to develop policies to make safer those PDAs, iPods, smart phones and USB flash drives used in business.

Lohrmann worries about the state's portable devices. He also worries about old equipment because he sees it everyday.

"The state has a lot," he said. "People don't realize a lot of old equipment can't be protected because it's not being supported (by the manufacturer) anymore. People think they're being penny-wise, but they're really being pound-foolish.

"You can't get security patches for Windows 97 or NT. There are no protections being written for that anymore, so when challenges come up, they're not protected."

That vulnerability is part of another worry — security-critical items often are cut when budgets are tight. And both government and private-business budgets in Michigan are very tight, Lohrmann noted.

"Zero Day attacks are the next big thing," Lohrmann said.

"People have firewalls, antivirus programs, and they don't realize there are new vulnerabilities coming up each day. You have to keep updating every day."

That's because people attempting to enter the system update their methods every day, he explained. They write software the security programs can't counter, such as computer worms. Sometimes they find a system vulnerability before anyone else does, and attack.

"It happened twice to the state — in February and again in March," Lohrmann said. "We were able to respond very quickly. There are procedural things you can do to protect yourself, but the things you think may be protecting you — such as antivirus programs — won't be."