



Computer security threats multiplying

BY JAMES MCNAIR | ENQUIRER STAFF WRITER

Corporations, insecure?

Yes, and increasingly under siege by threats against their information systems and intellectual property, three corporate security experts said this week at a half-day event sponsored by Xerox Global Services.

Insiders and outsiders, competitors and foreign countries, job-hunting older workers and tech-savvy new hires all represent challenges to companies with trade secrets, client lists and other information to protect, they said. David Drab, a 27-year veteran of the FBI who heads Xerox's Information Content Security division, said it is paramount to understand changing security risks.

"In today's world, I would suggest it's a cyber or virtual threat ... " Drab said to an audience of about 40. "We have not begun to comprehend the implications of this - the digitization of assets, the warp speed of technology and a business model that puts our intellectual property all over the globe ... Information is money, pure and simple, and if you've got it, somebody's going to go after it."

The experts - Homeland Defense Journal executive editor Dan Verton, Chicago intellectual property lawyer Mark Halligan and information security consultant Andrew Colarik - talked about the harm caused by hackers, crackers, cyber-criminals and cyber-terrorists.

"You are fleeced and don't even know you've been fleeced," Halligan said of companies that think they're immune to hackers. "When you leave your office on a Friday, everything's there and it's still there on Monday morning, but over the weekend, that information has been downloaded and transferred all over the world."

Of the problems coming from inside a company, Verton said, "you have two groups of individuals you really need to worry about - the criminally minded ... and the loyal, law-abiding employees who on a day-to-day basis are handling your sensitive information in a way that makes it vulnerable to inadvertent disclosure."

Companies, Verton said, need to adopt - and enforce - security policies, but must cope with younger employees accustomed to electronic liberties, not restrictions.

Colarik said companies must make tradeoffs between unfettered system usage and security.

<http://news.cincinnati.com/apps/pbcs.dll/article?AID=/20061019/BIZ02/610190323/1003/NEWS01>