

Into the (security) breach

By LESLIE STROOPE

June 8, 2006 – Crain's Cleveland Business

"Get ready — it's coming."

The information security breach at the Department of Veterans Affairs, which compromised the information of millions of Americans, was just the first wave of a giant digital tsunami headed straight for us, according to Cleveland-based author Andrew Colarik, who specializes in cyber-terrorism.

Dr. Colarik spoke at the Northern Ohio Information Technology Roundtable's summer meeting titled "Understanding Cyber Terrorism." The event drew more than 250 attendees from area banks, police departments, universities and technology consulting companies, according to Michael Dobeck, senior special agent with the electronic crimes task force in the U.S. Secret Service Cleveland field office.

Dr. Colarik spoke about securing the global information infrastructure against cyber-terrorist attacks.

For businesses, one of the most insidious — and prevalent — threats are "internal penetrations" into the infrastructure, coming from insider abuse motivated by revenge, financial gain or negligence, Dr. Colarik said.

"We are handing the keys to the insane asylum to the inmates," he said.

Dr. Colarik suggested two possible solutions to prevent these kinds of losses: management intervention and segmenting data so one person does not have access to all of a company's information. Dr. Colarik said rethinking the company's approach to security and then enacting those changes requires a "top-down approach with a bottom-up implementation."

However, Dr. Colarik said, changes need occur at both the macro level and the micro level.

On the macro level, he proposed sweeping changes to the global information infrastructure, such as eliminating the "open handshake" protocol, which is the foundation of all communication and security protocols, as well as creating a league of cyber communities, "like the league of nations," he said.

This league — comprised of the top 20 countries ranked by gross domestic product and Internet presence — would draft and enforce a treaty to establish information security standards.

He said the top 20 GDP countries control 80% of the world's wealth and 85% of the Internet.

Dr. Colarik also suggested making information a property right by delineating what is public and private, as well as creating a security industry underwriter's laboratory, similar to Underwriters Laboratories Inc., the nonprofit product safety and testing organization.

Dr. Colarik used a local analogy to illustrate the worldwide implications if changes aren't made to the infrastructure. He said the global information infrastructure threatened to become a digital Dead Man's Curve, where "to make a change (to the superstructure) is so expensive and so painful that it doesn't get done."



<http://www.crainscleveland.com/apps/pbcs.dll/article?AID=/20060608/FREE/60608010&SearchID=73247140010187>