The Miami Herald
Posted on Sun, Mar. 24, 2013

Enterprise Risk Management:Taking on the hackers

By Joseph A. Mann Jr.
josephmannjr@gmail.com

PATRICK FARRELL / MIAMI HERALD

Silka Gonzalez is founder and president of Enterprise Risk Management in Coral Gables. Tje company applies information security (anti-hacking) management systems and provides risk analysis for companies.

At the quiet offices of Enterprise Risk Management, a cyber security firm based in Coral Gables, paranoia is a driving force.

ERM is a small, expert group of information security and risk assessment consultants that is constantly guarding against people who are out to steal information or money and penetrate computer systems at financial institutions, government agencies, hospitals, universities and other enterprises.

“Hackers aren’t just kids playing from their homes,” said Silka González, a CPA and computer expert who is founder and president of ERM. “They are professionals hired by criminal organizations and by governments. I’m paranoid … We’re at the tip of the cybercrime iceberg,” said González, who has worked in IT security and auditing for more than 20 years at companies such as PricewaterhouseCoopers, Diageo PLC and the American Bankers Insurance Group (now known as Assurant Solutions).

She pointed to constant news stories about hackers — often based in Russia, China and North Korea — who penetrate United States government agencies, conduct widespread industrial espionage and sometimes steal information on millions of credit card holders. Other types of security breaches — like employees stealing USB drives containing confidential information, lax procedures for handling customer account inquiries at banks or failure to comply with complex federal regulations — can mean big financial losses for a company.

“Some companies don’t even realize they’ve been hacked until we investigate,” said González, who also is an assistant professor at Florida International University, where she teaches a graduate level IT audit course. “And some are ashamed to admit that they have.”

ERM, founded in 1998, provides a range of services designed to identify, prevent and control cybercrime and breaches in security. The firm provides computer network and wireless penetration tests (ethical hacking), emergency responses to hacker attacks, digital forensics to find out how and why an information security breach occurred, risk assessment, cloud security and auditing of IT systems.

The ERM founder, who grew up on a coffee plantation in Puerto Rico, was interested in business even as a child. “At eight, I was an entrepreneur, growing vegetables on a little plot at home and selling them at the public market," she said. González bought and repaired bicycles and raised three cows, which she later sold, to earn money. All this was to get enough money for a motorbike when she was around 12.

After earning bachelor's and master's degrees in computer information systems, González worked in IT security and auditing jobs at three large companies. Recognizing the importance of IT security, she decided to start her own company in Miami. "I got fed up with corporate life, took the $40,000 in my 401(k) account and started working alone from home," she said. González called some of her former clients and started out with contracts from Bacardi-Martini, FPL and Banco Internacional de Costa Rica.

The bilingual ERM president used her limited capital to develop a brochure for her fledgling company, start a Website and hire her first employee in 1999, a year after the company was set up.

Today, ERM has about 150 clients, González said, with a 95 percent retention rate. "We offer high-quality IT and security services," she added, "The big firms charge $200 or more per hour than we do." González declined to disclose revenue figures.

One of ERM's most sought-after skills is ethical hacking. "They pay us to hack into banks, airports and multinational companies," to test for weaknesses in their systems, said González, who has a full-time staff of 14, and offices in Washington, D.C. and India. "One time, we were able to hack into the e-mail of a CEO."

But when ERM is trying to hack into a bank or a company, "we have restraints," she added. "We can't break the law and we have a time limit. Illegal hackers don't have these limitations."

Esteban Farao, director of research and development at ERM, is an ethical hacker. Farao, a tall, well-dressed man who looks like he could be a college professor or a banker, described what he does when he attempts to penetrate a customer's IT system.

"When you go to war, you need to know your enemy," said Farao, who earned a bachelor's degree in information systems, an MBA and a master's degree in management information systems. First you have to do your research, looking at the website, checking out the target on Google, finding out as much as you can, and sometimes even searching through trash for clues, such as account numbers or pieces of a confidential memo, said the ERM executive, who has more than 15 years of experience carrying out attack and penetration projects and has worked with PricewaterhouseCoopers and several multinational companies. Farao studies a website thoroughly, identifying traffic patterns and looking for a weakness.

After the initial research, a hacker plans the next steps, he noted. Often, it's a question of testing a system to see if the people and procedures are sound.

For example, if the goal is to compromise a bank account, the hacker finds out how someone usually accesses the account — online, by phone or fax, and uses that information. A hacker may impersonate someone, phone a bank, say that he or she is traveling and has forgotten the password. "If the bank has sound security procedures in effect, the hacker is stopped. If not, the hacker may get some information and use that to build on — from obtaining a user ID to resetting a password," Farao said. "Small businesses are particularly vulnerable if they don't have a proper security in place."

ERM uses a portfolio of specialized computer programs, such as Qualys, Nessus and John the

Ripper in carrying out its penetration tests, and develops its own sophisticated programs in house. The company also carries out “social engineering tests” to probe the “human firewall” at companies. These tests may involve leaving a flash drive with supposedly sensitive information in an office to see if someone tries to steal it, or checking on whether employees are properly following security policies and procedures.

ERM’s clients come from a wide range of sectors and include: Banco Santander, Brightstar, Rinker Materials, Citibank, Banesco, Broward County, the State of Mississippi, Homeland Security and the U.S. State Department.

Mount Sinai Medical Center in Miami Beach, which runs a sophisticated IT system to protect the confidential patient information at its six locations, has been working with ERM for several years. “They perform penetration and vulnerability testing for us — they test our system to find gaps or weaknesses,” said Carlos Bitar, director of IT operations at the hospital, which has about 120 people in its IT department. ERM also helps the hospital ensure it is fully compliant with HIPAA (The Health Insurance Portability and Accountability Act), which sets strict standards for the security and privacy of patients’ data.

“They are very capable, very easy to work with, and they’re local,” Bitar added. “They provide great service.” The company is up to date on the latest IT technology, and they respond quickly when a problem arises, he added. “Even after a contract is over, I can call them and ask what other people in IT are doing, what are the best practices? And they don’t charge.”