LBC
LATIN BUSINESS CHRONICLE
latinbusinesschronicle.com
LATIN TRADE GROUP

Tuesday, April 01, 2014
Special Reports

The Cybersecurity Threat in Latin America

By Jerry Haar

Until last year, most Latin Americans felt that cybersecurity issues did not necessarily impact them. That all changed thanks to former NSA contractor Edward Snowden and revelations that the NSA monitored the communications of former Mexican president Felipe Calderón, current president Enrique Peña Nieto (when he was a candidate), and engaged in eavesdropping and electronic intelligence gathering in Brazil. Increasingly people began to realize: “If foreign governments can spy on my government, my government can spy on me and violate my individual right to privacy.” Add in the rapidly growing dimension of cybercrime (a greater, more immediate threat to individuals) and it becomes immediately apparent that cybersecurity is and will continue to be a huge policy issue in the Americas, as more of the population uses credits cards, shop online, or use any kind of electronic device that could steal their personal information

To put this in a global policy context, the first worldwide report, sponsored by McAfee and the defense think tank SDA, found that 57 percent of experts believe an arms race is taking place in cyberspace; more than one-third believe cybersecurity is more important than missile defense; 43 percent believe that critical threats to infrastructure (e.g., electric grid) is the greatest threat posed by cyber-attacks; and that the proliferation of smartphones and cloud computing are producing a whole new set of problems related to interconnectivity. The report concludes that a shortage of cyber workforce, a low level of preparedness for cyber-attacks, and only minor participation from industry in cybersecurity exercises give increasing cause for alarm.

As for Latin America and the Caribbean, the OAS white paper Latin American and Caribbean Cybersecurity Trends and Government Responses paints a very troublesome picture as well, particularly as it regards cybercriminals—the main threat to the average citizen. Citing an ESET Security Report, the white paper asserts that over half of businesses in LAC suffered cyber attacks in 2012—mainly malware, phishing and denial of service (a technique that floods computer networks with data to render websites functionless). This is particularly acute in Brazil, Mexico, and Argentina. Equally troublesome is pharming---redirecting traffic from one website to a fake website to steal information such as names and passwords. Throughout the region malware—mainly file infectors—plagues individuals and companies, as does spam and malicious URLs.

As pointed out in McAfee-SDA report, popular mobile devices and cloud are high-value targets. The Blackhole Exploit Kit, automatic transfer systems (in banking) and other tools have ballooned. Android malware rose from 1,000 to over 350,000 from 2011 to 2012 alone. Malware of all kinds, especially in banking increasingly plague the region, with cyber incidents growing from 12 percent to as high as 40 percent per year, as organized crime syndicates turn to the Internet to extort and launder funds

Online banking is the greatest, most common threat area. Criminals are always matching cybersecurity measures. If a bank uses a simple authentication system involving only a user name and password, keyloggers are used to gain access. Banks that use one-time password systems are injected with ATS scripts that hide illegal transactions. The BANCOS family of crime kits, with its online banking Trojans, is especially pernicious.

And not all the cybercrime devices are industrial country technology. Latin American hackers created a homegrown tool kit known as PiceBot for stealing financial information. Costing a mere $140, it is widely available for attacking customer accounts.

Cybercrime is expected to increase in the Americas, for cybercriminal organizations and networks are relentless. They configure their own servers in data centers worldwide, and they use free hosting services and trial services to register malicious domains. As the OAS reports: “Crimeware kits and the data they steal are commonly traded and shared on social networking sites.” Latin Americans are some of the world’s most active social media users.

Regional efforts to combat cybercrime are modest at best. Brazil is a case in point where there is a lot of talk but little action. While there are plans to create an anti-snooping email system, establish a funding pool for new ventures specializing in cybersecurity, and other preventive measures, to date there is no comprehensive policy or implementation of significant initiatives.

The challenges for Latin America are enormous. At present the region is hampered by inexperienced cybercrime investigators, a shortage of prosecutors specializing in technology-related offenses, not enough cybersecurity workers, and a public that is still relatively uneducated about cybersecurity. These must be addressed and corrected, with governmental strengthening of policy mechanisms and multilateral coordination throughout the Americas to effectively combat the growing spread of cybercrime. The technology exists through companies such as Easy Solutions and Catbird combat cybercrime. Whether Latin America will muster the resources, commitment and follow-through remain unanswered questions.

Jerry Haar is a professor of management and international business at Florida International University and a senior research fellow in the McDonough School of Business at Georgetown University.