Latin American Cyber and Security Risks

FEATURED EXPERT

James Bosworth, Founder, Hxagon

Cybersecurity issues in the United States and Europe may dominate much of media and multinationals' attention, but Latin America presents a different set of cyber risks that enterprises should take into account when doing business in the region. Just last week, Mexico's Central Bank announced that it is creating a dedicated cyber unit in the wake of a major attack in late April that siphoned tens or hundreds of millions of dollars from a domestic payments system used by the country's banks. Although hacking and surveillance techniques are not unique to Latin America, avenues of attack can vary from what other Western nations experience. To help understand how organizations can start to think about cybersecurity from Mexico to Chile, RANE spoke with James Bosworth of Hxagon. Highlights and key takeaways are featured below.

In some cases information taken from breached corporate networks has been used to help hijack trucks. Likewise, there have been several examples of criminal gangs in infiltrating company systems or devices to help track executives for the purpose of extortion, kidnapping, or robbery.

An Alarming Lack of Transparency

While regulators in the United States and Europe push for greater disclosure from organizations that have been hacked or subjected to data breaches, equivalent coordinated efforts do not exist in Latin America — and the lack of disclosure itself presents a formidable risk. James Bosworth says that "a big red flag is the sheer lack of acknowledgement" surrounding cyberattacks and hacking attempts. "If you're an oil company or power utility in the U.S., you know you're being hacked. There are attacks coming in from all sorts of vectors. Everybody knows that they're being hacked by non-state actors." Yet throughout Latin America, "there's basically no acknowledgement" that hacks are taking place.

As part of that, there is little in the way of public information about infiltrations or successful attacks. Without such discussions and the information sharing that often accompanies them, organizations have little true understanding of the scope of the threat landscape. "In a lot of cases, we don't know the threats. The lack of formal information sharing — who and what's been hit — is a vulnerability in itself," Bosworth argues. "There are not public examples of companies losing their trade secrets, so people are not so worried about it."

A relatively large number of Latin American firms did claim in an Organization of American States (OAS) survey that they participate in informal working groups to share threat information. But Bosworth says these are "barely scratching the surface" in terms of information sharing, and ***he suggests that U.S. and other foreign firms operating in the region start their own, more sophisticated threat intel group efforts.*** "They should take the current lack of structure as a chance to shape and improve the security landscape."

Despite that lack of transparency, it's clear that hackers are busy at work in Latin America. ***There are a few Brazilian hacker groups that operate across borders, particularly those that go after banks, and Brazilian-written malware is sometimes altered to be used in other countries, according to Bosworth.*** Criminal organizations in the region that deal in credit card theft and money laundering also have connections with Eastern European and Russian hackers. While publicly acknowledged instances of nation-state actors like Russia, China and Iran targeting companies or critical infrastructure in Latin America are few and far between, it's hard to believe that they wouldn't do so given their well documented campaigns in the U.S. and Europe.

James Bosworth advises enterprises to monitor government surveillance attempts. For the most part, Latin American governments have attempted to target political opponents and not private institutions, though that could change.

Governmental Resources Not At the Ready

On the regulatory and enforcement front, there are some modest cyber efforts in the region. The OAS has developed "a pretty decent cybersecurity initiative," including documenting best practices and helping countries in the hemisphere set up computer emergency response teams (CERTs). ***But the country-specific CERTs are relatively reactive in nature.*** And though those in bigger, more advanced nations (and the biggest cyber targets) like Brazil, Mexico and Argentina do attempt to track risk in certain sectors, they don't compare to the critical protection efforts like that of the U.S. Department of Homeland Security. "None are a shining example for how this should be done," Bosworth says.

Even more troubling, the situation is unlikely to change drastically. "Latin America has other priorities," Bosworth cautions, noting that Mexico has a homicide rate north of 20 per 100,000 people. "It's hard to devote the resources necessary for cyber threats."

Hybrid Threats: Online Information and Physical Safety

From an enterprise standpoint, much of the focus around security in Latin America remains on physical safety. The rising crime rate over the past few years in certain countries, such as Mexico, Brazil and Venezuela, often means that organizations will be much more aware of and willing to spend money against the greater relative risk, such as armed robbery over cyberthreats. Yet the connections between the two might be stronger than many companies appreciate. In some cases, Bosworth says, information taken from breached corporate networks has been used to help hijack trucks. ***Likewise, there have been several examples of criminal gangs infiltrating company systems or devices to help track executives for the purpose of extortion, kidnapping, or robbery.***

Bosworth notes that many executives will avoid taking their personal electronics, such as mobile phones or laptops, to certain high-risk areas for cybercrime, such as Russia or China. However, those same executives don't think twice about taking them to Latin America, where the danger of being hacked exists, even if it is less documented.

The prevalence of physical crime throughout the region is connected to cyber-related risk in other ways. It is highly probable that company employees in Latin America could be robbed of their mobile devices at some point. "If your company email is on that phone, you have to consider what access employees have." ***Bosworth recommends that enterprises install ways to block access or perform a remote wipe of the smartphone's contents.***

The Prevalence of Spyware and Malware

"Voice communications have been very heavily tapped" across Latin America, Bosworth says. ***It is therefore imperative that businesspeople use at least a basic level of encryption for phone calls and text messages, like that offered by apps such as Signal or WhatsApp.*** If these applications are used, the chance of falling victim to eavesdropping efforts is "virtually nil — assuming they haven't compromised your phone," he maintains.

"Latin America gets scams we don't see in the U.S.," Bosworth stresses, adding that criminals have been known to launch spyware unique to the region. One widespread scam took advantage of news surrounding late Venezuelan leader Hugo Chávez's failing health: Automated bots would disseminate links promising health updates but spreading malware instead — something that happens throughout Latin America when major news breaks, according to Bosworth. ***"Training local staff not to click — that is critical in Latin America."***

Yet while WhatsApp is very useful for guarding against eavesdropping, its "absolute dominance" of messaging apps in many Latin American markets can create other problems. "We [in the U.S.] don't think of WhatsApp as much of a major platform, but the scams you see in places like Brazil and Mexico are hitting WhatsApp first," Bosworth says. "Getting a handle on the WhatsApp scams is critical for Latin America."

Bosworth explains that criminals are also targeting websites with two-factor authentication (2FA), developing them "in parallel to the ones you're seeing in the U.S." It's important to know what those attacks look like. "If a website is hijacked, it sends a link to phone and can send malware" as part of the 2FA process.

Just as in the U.S. and Europe, elections are fast becoming a favorite target of hackers, and this year will see several major votes including in Colombia, Mexico and Brazil. According to Bosworth, Latin America has its own media-manipulation issues, evidenced in armies of automated social media bots looking to stir up domestic turmoil focused on Honduras and Mexico, among other countries. Russia is one state actor potentially meddling in the region's elections.

Pirated Software and Third-Party Vendors

Pirated software is prevalent in Latin America, resulting in computers and servers running programs and systems without the necessary security patches. One example found in Peru involved counterfeit software used by architectural firms that covertly sends data to servers in China. "The poorer the country, the higher the incidence of hacked software will be," Bosworth notes. The threat increases with the use of third-party vendors that might also be using pirated software. ***As a result, global cyber-events such as the WannaCry attack in May 2017 usually also affect Latin American nations***, as well as those in Southeast Asia and Africa, even if news coverage doesn't always reflect that. Hospitals in Colombia were affected along with those in the UK, further evidence of just how important it is to monitor global cyber events rather than have a more limited, regional perspective.

Monitoring Government Surveillance Efforts

Bosworth advises enterprises to monitor government surveillance attempts. For the most part, Latin American governments have attempted to target political opponents and not private institutions, though that could change. "It's not the biggest threat to corporations — until it is." Governments in Venezuela and Mexico have established surveillance programs, for instance. "It's not a day-to-day issue for most companies, but the fact that governments are doing that should be a concern," as government spyware "could very easily get into their employee networks as well," he warns.

While there aren't solid examples of governments tracking corporations or their employees in Latin America, a state sponsor of cyber-espionage might see private enterprise as "a tempting vulnerability — and it wouldn't be disclosed by anybody," Bosworth concludes.

"The lack of formal information sharing — who and what's been hit — is a vulnerability in itself," James Bosworth argues. "There are not public examples of companies losing their trade secrets, so people are not so worried about it."

ABOUT THE EXPERT

James Bosworth *writes and consults on politics, security, economics, and technology issues in emerging markets, particularly Latin America and the Caribbean. He is the founder of Hxagon, LLC.*

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.