Executive Summary

Latin America is vulnerable to hostile cyber activity, especially as the region develops economically and technologically. As the region's economies become more technically adept, cyber security practices are currently failing to keep up with advancements in digitization. Cyber crime, cyber espionage, and hacktivism have all targeted Latin America. Mexico in particular is one of the fastest growing economies in the world, leveraging technology to propel business forward. Mexico is on pace to be among the top ten economies in the world by 2050, which is largely the result of increased Internet access and implementation of e-commerce. As such, Mexico has been attracting the attention of enterprising hostile cyber actors seeking to exploit commercial organizations for financial reward. While promising initiatives like the establishment of a national cyber security strategy and legal frameworks demonstrate Mexico’s awareness of the importance of cyber security, they are at a nascent stage; it remains to be seen how they will be implemented, socialized, and enforced. LookingGlass analysts expect Mexico to continue to be a prime target in the region, particularly as its cyber security efforts are in the unenviable position of playing catch-up to its economic development.

Key Points

- Mexico is one of the leading emerging economies in the region and, as such, will continue to garner the attention of hostile actors to exploit vulnerable in-country organizations. Banks and financial institutions have been the primary targets of hostile actors.

- Cyber crime is the primary threat, which should continue for the foreseeable future. State-driven cyber espionage has been observed targeting Mexican interests. Such activity largely depends on the intent of actors seeking to ascertain the Mexican government’s position on geopolitical issues and will ebb and flow accordingly. Hacktivism is a viable means of social protest that has historically targeted government entities and will likely continue in the future.

- Unfortunately, there is limited information kept by government organizations to provide more fidelity on hostile cyber activity statistics. That said, current Mexican law does not mandate that organizations report breaches, making those statistics -- even if they were available -- unreliable.
Latin America

As a region, Latin America is facing an increasing amount of cyber attacks. A primary reason for this is its growing population, which is increasingly connected to the Internet, as well as the developing digitization of its regional economies. The four largest economies – Argentina, Brazil, Colombia, and Mexico – are most at-risk, along with some smaller economies that excel in technological innovation, such as Peru. Further complicating the situation, Latin America/the Caribbean is the 4th largest mobile communications market in the world; it is estimated there will be more than 600 million connected smartphones in this region alone by 2020. Mobile penetration has grown rapidly over the last three years, with 41 percent of transactions in the network now originating from a mobile device, up from just 12 percent in the same quarter three years ago. Cyber attacks against mobile devices continue to be on the upswing, and it follows that such activities would target Latin American mobile customers as well.

In 2016, the Inter-American Development Bank (IDB) and the Organization of American States (OAS) sponsored a report on the status of cyber security in Latin America. The findings indicated that the region was very vulnerable to cyber attacks, with four in five states not having viable cyber security strategies or plans for protecting critical infrastructure in place. Two in three lacked any sort of command and control center for cybersecurity crises. Enforcement of laws against cyber attacks was almost universally weak. Overall, the entire region is being exploited by hostile attackers, largely due to the following reasons (according to the IEEE):

- **There are few coordinated defense mechanisms.** Many Latin American countries are beginning to develop Cyber Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to handle attacks.

- **Public awareness is lacking.** Many Latin American countries have not yet publicized the dangers of the Internet. Private industries also frequently believe that they are not targets, so they have not made preventative programs a high priority.

- **There is a disconnect between public and private industries.** Stakeholders have yet to develop enough trust to collaborate, and most Latin American countries are lacking reputable clearinghouses or brokers of authoritative information to allow the establishment of formal information-sharing mechanisms.

As a region, the annual cost of cyber crime in Latin America – to include Caribbean nations – has grown to USD 90 billion a year, according to a 2016 report by the IDB. Overall, the IDB found that the region was increasingly susceptible to severe cyber incidents; this is partly attributed to the fact that many computer security companies have not traditionally viewed
Latin America as a prime market for their products and services. In order to combat this perception and ameliorate the situation, in April 2017, the OAS passed a resolution to increase cooperation and stability in cyberspace, raising cyber security awareness and fostering information-sharing amongst the regional governments. Other challenges exist, making cyber security an ongoing uphill battle -- to include a lack of qualified individuals and a dearth of cyber insurance offerings in the region.

**Mexico**

Mexico is the 15th largest economy in the world. In the Latin American region, Mexico’s gross domestic product is second only to Brazil’s. Such a potent economic standing is an attractive target for enterprising criminals. According to a think tank’s reporting, Mexico enjoys considerable Foreign Direct Investment, registering an 11 percent increase from 2014-2015, or USD 28 billion in 2015. Such investment and the presence of foreign companies in Mexico represent both a positive economic progression and the potential for targeting by hostile cyber actors. According to at least one source, Mexico ranks second behind Brazil for being victimized by the most cyber attacks, with banking, retail, and telecommunications being the most targeted sectors. Figure 1 shows the Top 20 countries facing the highest threat levels in 2015.

![Figure 1. Top 20 Countries Facing the Highest Threat Levels in 2015](source: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/2015-09-09-cyber-mexico-whitepaper-WEB.pdf)
This is a concern given that Mexican cyber security efforts appear to remain nascent. According to a report from an international consulting firm, as of mid-2016, Mexico was still in an immature state of cybersecurity due to a lack of investment in cyber crime protection. In the previous 12 months, Mexico had just over three million security incidents, with around 87 percent of companies experiencing some form of privacy breach. This was 13 percent higher than the global trend at the time. On a worldwide scale, the average cost of a single cyber crime incident was $2,386,719, compared to $1,581,641 in Mexico.xv

According to a think tank report on the cyber security landscape in Mexico, the Scientific Division of the Federal Police stated that there was a 300 percent increase in cyber incidents from 2013 (30,000 incidents reported) to 2016 (60,000); computer virus deployment increased 57 percent between 2015 and 2016.xvi The same think tank report revealed that the majority of cyber fraud occurred via Internet transactions through e-commerce and mobile banking.

**Cyber Threat Actor Landscape**

The cyber threat landscape consists of diverse hostile actors with various intent, capabilities, and motivations for launching operations. States, cyber criminals, and activists are the primary actors that are launching attacks against entities in Mexico, as shown in Figure 2 below.

![Figure 2. Percentage of Actors Behind Cyber Activity in 2015](source: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/2015-09-09-cyber-mexico-whitepaper WEB.pdf)
State Actors

Nation states are largely considered the most sophisticated actor set; they have the capabilities to exploit networks for data theft or manipulation or to launch attacks to disrupt, deny, degrade, or destroy information systems or the information resident on them. State actors are generally behind cyber espionage activities, although industrial cyber espionage (where a company targets another company) also occurs. State actors and/or state-directed actors target public and private sector entities for a variety of reasons, such as the theft of intellectual property, research and development, merger & acquisition data, trade secrets, and business strategies. However, as detailed in the bullet points below, state actors have also been observed conducting cyber attacks to simply steal money, illustrating how the motives of hostile cyber actors are blurring.

- **North Korea.** Suspected North Korean hackers attempted to steal money from Mexican banks in 2016. The hackers ended up deploying destructive malware after they had unsuccessfully exploited the SWIFT payment system to steal money via fraudulent transfer requests. In 2017, more than 500 companies in Mexico were infected with the WannaCry ransomware, believed to have been orchestrated by North Korea.

- **Mexico.** In 2017, the Mexican government was implicated in an attack in which surveillance spyware was deployed on journalists’ and activists’ smartphones.

- **Russia.** Russia is actively seeking to expand its influence in Latin America in order to offset U.S. influence in the region. Given Russia’s involvement in elections in the United States and Europe, similar social media influence operations are believed to have occurred in Latin American political elections. According to one vendor report, Russian operatives are believed to have conducted cyber espionage against Government of Mexico targets, although no specifics were provided.

- **Careto APT.** In 2014, the Careto APT group was detected targeting many unnamed organizations in Latin America in order to obtain strategic financial and economic information.

Cyber Crime

Cyber criminals’ endeavors run the gamut of sophistication, ranging from rudimentary to very refined, and are conducted by organizations of various sizes, from individuals to teams to large groups. The span of operations is as diverse as the actors themselves, with targets ranging from individuals to businesses to healthcare organizations to financial institutions. Moreover, like all actors in cyber space, they are not contained by geographic boundaries and operate globally. Latin America is home to its own cyber criminal
underground, which has grown over the past few years. According to a computer security company, weak regional cyber security awareness, limited information-sharing mechanisms between private and public sectors, and a generally uninformed public enable cyber criminal activity.\textsuperscript{xiii}

In 2016, cyber crime cost Mexico an estimated USD 3 billion in economic damages.\textsuperscript{xxiv} In 2015, a computer security vendor estimated that cyber crime cost companies in Mexico approximately US 5.5 billion. During this time, five out of six large corporations and 60 percent of small-to-medium enterprises were victims of online attacks, per the security vendor’s findings.\textsuperscript{xxv} Discrepancies in these costs is a testament to how such figures are estimates at best and reliant on factors such as accurate reporting. Regardless, cyber criminals have demonstrated their capabilities against the Mexican financial sector by exploiting ATMs and defrauding bank customers, while also employing such tactics as using banking Trojans, launching ransomware attacks, and deploying point-of-sale malware.\textsuperscript{xxvi} Figure 3 shows how Mexico compares with other countries with respect to consumer loss as a result of cyber crime.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{consumer_loss.png}
\end{figure}

\section*{State Activity or Cyber Crime?}

A computer security company revealed a campaign that has been targeting users in Mexico since as early as 2013.\textsuperscript{xxvii} Per the company’s findings, the campaign has leveraged spear phishing e-mails and USB devices to gain access to victims’ devices. The malware consisted of multi-modules: one to ensure the malware ran properly; one that served as an
information-stealer taking saved passwords from web browsers and e-mail and FTP clients; one that served as a keylogger; one responsible for communicating with the command-and-control server; one that infected USB drives; and one that stole credentials from online banking sites and reservation systems.

At present, there hasn’t been any attribution to the classification of actor behind this campaign, although the company’s researchers described it as “unusually sophisticated.” The company’s researchers noted that the actors behind this campaign did closely monitor the operations, although the particulars were not shared.

Such activity is indicative of the continued confluence of cyber crime and cyber espionage campaigns, as they continue to use the same tactics, techniques, and procedures (TTPs). Since many of these TTPs share similar characteristics, attribution efforts rely heavily on visibility of the target’s attack surface to assist in determining attacker motivation. While in some instances the target’s identification greatly aids this effort, it is not foolproof. Case and point, North Korea and now Iran have been suspected in conducting hostile cyber activity typically associated with cyber criminals by stealing money from financial institutions and cryptocurrency repositories using the TTPs implemented by cyber espionage actors.xxviii, xxix, xxx In this example, it is reasonable to suspect potential state actors are targeting the banks for the same reason that cyber criminals would – for financial gain.

Hacktivism

Hacktivism melds traditional political activism with the Internet, allowing these groups and individuals to express social and political discontent via cyberspace rather than in person or to use digital tools to pursue political objectives. Because the hacktivist landscape is diverse in its own right, encompassing numerous individuals and groups representing varied political, religious, economic, and environmental constituencies, it is difficult to highlight each group with any fidelity. For example, the hacktivist group “MexicanH Team” claimed to have accessed the databases and servers of the Mexican army, navy, and the ruling party, as well as network giant Televisa.xxii Hacktivism in Mexico started in the late 1990s with the emergence of the Electronic Disturbance Theater and has since largely centered around political and social causes, as illustrated in some of the examples below. However, targets correspond with causes and, as such, are subject to change.

- In June 2018, unknown hackers launched a distributed denial-of-service attack on a website opposing a Mexican presidential candidate of the National Action Party. Most of the network traffic originated from China and Russia. As of this writing, it is uncertain who was behind the attack.xxxii

- In 2016, the independent online TV portal Romperviotttov.com was targeted by a DDoS attack that impacted its operations for several days.xxxiii
• In 2014, Anonymous Mexico conducted defacements against Mexico’s Ministry of Defense website.xxxiv

• In 2012, Mexican hacktivists targeted governmental infrastructures that supported presidential elections utilizing DDoS attacks, web page defacements, cross-site scripting, and SQL injection.xxxv

• In 2011, Mexican hacktivists joined the Anonymous hacking enclave’s operation #OpCartel in order to publicize sensitive data about Mexican criminal organizations.xxxvi

Who are the Targets?

Banking, retail, and telecommunications are the top targets in Mexico. In 2016, a survey of local and multinational firms based in Mexico was conducted; during the 2015-2016 reporting period, virtual extortion (such as via ransomware) was the top private sector security incident for those polled at 49 percent.xxxvii Unsurprisingly, according to one report, in 2015 financial institutions and information assets were primary targets based on attack vector. Point-of-sale malware, advanced persistent threat activity, unauthorized access, and DDoS attacks rounded out the top five (see Figure 4).

![Figure 4. Most Common Attack Vectors Targeting Mexican Organizations in 2015](source: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/2015-09-09-cyber-mexico-whitepaper WEB.pdf)

These findings are consistent with another report conducted in 2016 by an international consulting firm, which found that 87 percent of Mexico-based companies experienced a
cyber attack over the previous 12 months, resulting in approximately three million incidents.xxxvii

Financial Sector/Banks are Top Targets

According to one think tank, despite being the most protected sector, the financial sector in Mexico is the most targeted, facing extortion attacks, disruption of trading platforms, and DDoS attacks, among others.xxxix In 2018, banks in Mexico have been increasingly targeted by cyber criminals. At the end of April 2018, Mexico’s financial system was the victim of a cyberattack in which cyber criminals stole approximately USD 20 million. At least five banks had recorded large withdrawals of money through unauthorized transfers to bogus accounts.xl This recent activity reveals that cyber criminals have the capability to successfully target financial institutions and will likely do so for the foreseeable future, particularly if the environment is favorable to their operations. According to one researcher, moving money internationally out of Mexico is difficult due to strict foreign exchange controls and the extensive approval processes required. As such, these type of schemes would require an extensive in-country team, including money mules to withdraw fraudulent funds, which points to the culprits of this case being in-country hackers.xli

Cyber Security in Mexico

Despite taking promising steps, Mexico still has a weak cyber security posture that needs improvement. According to the International Telecommunications Union, a United Nations specialized agency for information and communication technologies, Mexico’s measure of cyber security readiness index ranked it 28 out of 195 countries in 2017. The report covers five categories, to include Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation.xlii Mexico was third in the Americas (behind the United States and Canada).

National Cyber Security Strategy

Mexico’s National Cyber Security strategy was developed in collaboration with the Inter-American Committee against Terrorism. The strategy underscores Mexico’s commitment to combatting cyber crime and recognizes the importance of information and communication technologies in Mexico’s political, social, and economic development.xliii Per a think tank review of the strategy, three governing principles – human rights, risk management, and multi-disciplinary cooperation – anchor the document in support of five strategic objectives: society and rights; economy and innovation; public institutions; public safety; and national security.xliv With the implementation of this document, Mexico joins six other Latin American countries in establishing a national cyber security strategy: Colombia (2011 and 2016),

Cyber Crime-Related Laws

There is no definition for “cyber crime” and “cybersecurity” in Mexican legislation, and Mexico has not yet adopted international standards applicable to cyber crimes. While Mexico scored high in having criminal and data privacy legislation on the books, organizations are not required to have a minimal set of cybersecurity measures in place, nor are they required to report incidents to authorities, which make harvesting hostile cyber statistics difficult to measure. According to a U.S. think tank, as of 2017, Mexico had not enacted specific legislation on cybersecurity, though it was included in the Federal Criminal Code, mostly regarding financial crimes, information security, and the use of technology in other crimes, such as terrorism, kidnapping, and drug trafficking. Furthermore, to demonstrate legislation’s limited deterrence capability, as of 2016, theft of personal and business data in Mexico via hacking had been noticeably increasing, with Mexico becoming a haven for the black market of stolen personal data.

Conclusion

Mexico’s increasing posture as a regional economic player will continue to garner hostile cyber actor attention. Cyber criminals continue to be the major threat facing organizations in Mexico, although state actors have demonstrated an interest in Latin America via cyber espionage campaigns. Hacktivism remains politically-focused; any perceived social injustice can easily motivate these online activists to target any organization in any sector. Mexico’s establishment of a national cyber security strategy is an important milestone in demonstrating the government’s understanding of the potential threats that exist in cyberspace and places Mexico in the company of six other regional governments with similar strategies. However, while legislation exists that addresses technology-related crime, Mexico’s failure to incentivize or compel organizations to report breaches, makes it difficult to understand the full impact of hostile cyber activity in the country. This needs to change in order to develop proper cyber security initiatives to adequately address these criminal activities.

There is little anecdotal reporting highlighting the cyber security posture of and threats facing foreign companies in Mexico. Based on available reporting, financial-related organizations are likely desirable targets for enterprising criminal groups. Cyber espionage extends beyond nation states, and commercial competitors may leverage network exploitation to obtain sensitive data such as research and development; business planning and operations; mergers and acquisitions; or future strategies. For state actors, aside from
those believed to be targeting global financial institutions for profit, targeting will likely ebb and flow depending on the intent of those governments orchestrating it.
# Traffic-Light Protocol for Information Dissemination

<table>
<thead>
<tr>
<th>Color</th>
<th>When Should It Be Used?</th>
<th>How May It Be Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED</td>
<td>Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party’s privacy, reputation, or operations if misused.</td>
<td>Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</td>
</tr>
<tr>
<td>AMBER</td>
<td>Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries the risks to privacy, reputation, or operations if shared outside of the organizations involved.</td>
<td>Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.</td>
</tr>
<tr>
<td>GREEN</td>
<td>Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</td>
<td>Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publically accessible channels.</td>
</tr>
<tr>
<td>WHITE</td>
<td>Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>TLP: WHITE information may be distributed without restriction, subject to copyright controls.</td>
</tr>
</tbody>
</table>
A Note on Estimative Language

Estimative language is used in order to convey an assessed likelihood or probability of an event, as well as the level of confidence ascribed to a judgment. Assessments are based on collected information (which is often incomplete), as well as logic, argumentation, and precedents. Confidence levels provide assessments of the quality and quantity of the source information that supports judgments.

<table>
<thead>
<tr>
<th>Confidence Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>Totally reliable and corroborated information with no assumptions and clear, undisputed reasoning.</td>
</tr>
<tr>
<td>High</td>
<td>Well corroborated information from multiple proven sources, extensive databases, and/or a deep historical understanding of the issue. There are minimal assumptions present. The analytic reasoning is dominated by logical inferences developed through established methodology or multiple analytic techniques. High confidence does not imply an assessment is fact or a certainty.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Partially corroborated information from sufficient quality sources (a mix of proven and unproven sources) with some databases and/or historical understanding of the issue. There are assumptions present, of which some should be crucial to the analysis. Reasoning is a mixture of strong and weak inferences developed through simple analytic techniques or an established methodology.</td>
</tr>
<tr>
<td>Low</td>
<td>Uncorroborated information from good or marginal sources (mix of semi-proven and unproven sources) with minimal database or historical understanding of the issue. There are many assumptions critical to the analysis. Reasoning is dominated by weak inferences through few analytic techniques.</td>
</tr>
<tr>
<td>None</td>
<td>There is no direct information or partially corroborated information to support analytic assessments or judgments, or it is exploratory analysis.</td>
</tr>
</tbody>
</table>
Source and Information Reliability

Source

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Reliable</td>
</tr>
<tr>
<td>B</td>
<td>Usually Reliable</td>
</tr>
<tr>
<td>C</td>
<td>Fairly Reliable</td>
</tr>
<tr>
<td>D</td>
<td>Not Usually Reliable</td>
</tr>
<tr>
<td>E</td>
<td>Unreliable</td>
</tr>
<tr>
<td>F</td>
<td>Can't Be Judged</td>
</tr>
</tbody>
</table>

Description

A
No doubt about the source’s authenticity, trustworthiness, or competency. History of complete reliability.

B
Minor doubts. History of mostly valid information.

C
Doubts. Provided valid information in the past.

D
Provided valid information in the past.

E
Lacks authenticity, trustworthiness, and competency. History of invalid information.

F
Insufficient information to evaluate reliability. May or may not be reliable.

Information

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Confirmed</td>
</tr>
<tr>
<td>2</td>
<td>Probably True</td>
</tr>
<tr>
<td>3</td>
<td>Possibly True</td>
</tr>
<tr>
<td>4</td>
<td>Doubtfully True</td>
</tr>
<tr>
<td>5</td>
<td>Improbable</td>
</tr>
<tr>
<td>6</td>
<td>Can't Be Judged</td>
</tr>
</tbody>
</table>

Description

1
Logical, consistent with other relevant information, confirmed by independent sources.

2
Logical, consistent with other relevant information, not confirmed by independent sources.

3
Reasonably logical, agrees with some relevant information, not confirmed.

4
Not logical but possible, no other information on the subject, not confirmed.

5
Not logical, contradicted by other relevant information.

6
The validity of the information cannot be determined.


https://www.welivesecurity.com/2018/05/24/mexico-cybercriminals-steal-400-million/

https://www.bankinfosecurity.com/mexico-investigates-suspected-cyberattacks-against-banks-a-11008


Ibid.

https://portswigger.net/daily-swig/mexico-launches-national-cyber-security-strategy


Ibid.

https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf