CYBER THREAT ANALYSIS

Recorded Future®

Insikt Group®

June 25, 2026

Evaluating Mexico's New Cybersecurity Plan

Mexico's newly announced National Cybersecurity Plan is a timely response to cyber threats in the country, and it lays out a path for stronger national coordination.

The Plan addresses some of Mexico's main cyber threats, which are primarily ransomware, financial malware, fraud, and hacktivism, followed by data theft, organized crime, money laundering, and state-linked activity.

The 2026 FIFA World Cup will test Mexico's cyber posture, making threat detection, incident response, and public cyber safety training urgent priorities as implementation of the Plan moves ahead.

Executive Summary

Mexico recently unveiled a new National Cybersecurity Plan to be implemented over the remainder of this decade. The proposed plan lays the foundation to address the top cybersecurity threats Mexico has identified, including organized crime, geopolitical threats, and emerging artificial intelligence (AI) threats. The plan comes at a critical moment, as repeated cyber incidents across federal, state, and local institutions in Mexico have exposed the need for a more coordinated national response to reduce the risk of data theft, ransomware, service disruptions, and institutional reputational damage.

Insikt Group analysis of cyber trends from 2020 to 2026 found that Mexico has historically been primarily impacted by ransomware, financial malware and fraud, and hacktivism. Data breaches and theft, organized crime and money laundering, and state-sponsored cybercrime have also represented significant threats. The government, healthcare, and financial sectors have been the primary targets of cyber threat actors, and ransomware continues to be the top threat to Mexican organizations. Mexico also remains an attractive target for state-sponsored cyber activity due to its deep integration with United States (US) supply chains, nearshoring-linked manufacturing base, and underdeveloped cybergovernance.

Mexico is among the top five countries globally with the most documented victims of infostealers and stolen payment cards. Our research indicated that DarkForums is the most popular dark web special-access forum where threat actors discuss cyberattacks targeting Mexico. Mexican drug trafficking organizations (DTOs) are known to leverage Chinese money laundering networks (CMLNs) for their drug proceeds, relying on cryptocurrency to obfuscate their flow of illicit funds and soliciting cybercrime-as-a-service to evade arrests.

The ongoing 2026 FIFA World Cup, co-hosted by Mexico, will be an initial test of the country's ability to maintain operations and access to digital services amid increased tourism and international scrutiny. Facing this dynamic, organizations in Mexico should enhance their ability to detect cyber threats, prioritize threat visibility, and strengthen incident response planning. They should also train staff and the public on basic cyber safety, with an emphasis on building a practical understanding of how to respond quickly and effectively when incidents occur.

Key Findings

- Mexico's proposed National Cybersecurity Plan outlines a path to update the country's cyber posture at a critical moment. While previous attempts to advance national cybersecurity policy failed to get political traction, the administration of President Claudia Sheinbaum has committed to fully implementing this initiative over the course of her term, facilitated by her party's majority control of Congress.
- In addition to the threats outlined in the plan, Insikt Group assesses that Mexico faces significant challenges related to ransomware, financial malware and fraud, and hacktivism. Data breaches and theft, organized crime and money laundering, and state-sponsored cyber threats also continue to pose a major challenge.
- As Mexico advances its new cyber policy, organizations operating in the country should consider strengthening their threat posture by leveraging cyber threat intelligence solutions, adopting international cyber standards, conducting scenario-planning exercises to improve responses to ransomware, data breaches, cyber espionage, and other threats, and educating employees and the general public.

Mexico's Cybersecurity Positioning

On December 4, 2025, Mexico's 2025–2030 National Cybersecurity Plan (hereinafter, the Plan) was published by the Mexican Digital Transformation and Telecommunications Agency (ATDT). The Plan is meant to update Mexican federal cyber policy for today's threat environment and to create a more secure and resilient digital security policy ecosystem. While the Plan by itself does not create new cyber policies or legal frameworks, it outlines a series of benchmarks and indicators to guide progress toward that end. Ultimately, as the ATDT claims in the Plan, it is an attempt by Mexico to become a regional cyber-leader. Mexico was listed as a "Tier 2" nation in the International Telecommunication Union's (ITU) 2024 Global Cybersecurity Index, placing it alongside Canada, Ecuador, and Uruguay in the upper ranks of Latin American nations for demonstrating a strong commitment to cybersecurity (Brazil and the US are the only countries in the Americas listed in Tier 1). However, the ITU identifies international cooperation as an area of growth, and Mexico is generally perceived by cyber experts as lagging behind international standards in institutional capacity-building. When implemented, the ATDT claims that the Plan will "position Mexico at the forefront of regional cybersecurity, contributing not only to the protection of its own digital assets and population but also to the strengthening of regional cybersecurity in Latin America and the Caribbean."

The Plan comes at a crucial time for cybersecurity in Mexico, after several high-profile cyber incidents that have highlighted the need for greater resilience and coordination. In recent years, federal institutions have faced serious breaches and disruptions, including a high-profile 2022 hacktivist leak of sensitive files from Mexico's Secretariat of National Defense (SEDENA), a 2022 ransomware attack on the Secretariat of Infrastructure, Communications, and Transportation (SICT), a 2023 BlackByte ransomware attack against the National Water Commission (CONAGUA), and a 2024 RansomHub attack affecting the Legal Counsel's Office of the Presidency. State and local institutions have also faced reported or suspected incidents, including the 2024 exposure of Mexico City government emails and a 2025 intrusion involving Yucatán's Va y Ven transit system. These incidents show that Mexico's cyber risks are not limited to a single agency or sector, and that a fragmented, uncoordinated national response capacity can leave public institutions vulnerable to data theft, service disruptions, ransomware, and reputational damage.

Mexico's 2025–2030 National Cybersecurity Plan outlines a gradual, stepwise approach to updating the country's cyber capabilities over the next six years. This includes:

- **2025 — Foundation Phase:** The Plan's implementation began with the publication in December 2025 of a general cybersecurity framework establishing responsibilities, governance mechanisms, risk-management expectations, incident reporting procedures, vulnerability management, training and awareness measures, and coordination plans. After launching the framework and the Plan, the ATDT has shared both across Mexican federal agencies and international partners. As part of this stage of the Plan, Mexico also formally joined the Latin America and Caribbean Cyber Competence Centre (LAC4) and signed a Memorandum of Understanding (MOU) with Brazil on cybersecurity matters.

- **2026 — Expansion Phase:** This phase, which the ATDT describes as currently ongoing, includes developing and announcing a new National Cybersecurity Strategy by the third quarter of 2026, passing a new General Cybersecurity Law in Mexico's legislature, and creating a National Center for Cybersecurity Operations to continuously monitor threats, correlate security events across federal institutions, and detect cyberattacks early. This stage of the plan also calls for integrating a wider network of public, private, academic, sectoral, and international computer security incident response teams (CSIRTs); identifying critical infrastructure and essential services; creating a federal vulnerability assessment program; launching a Federal Virtual Academy to support implementation of cybersecurity policies and guidelines; establishing the National Cybersecurity Contact Network (RNCC-MX); signing additional bilateral and CSIRT-related MOUs; developing a federal computer emergency response team (CERT)/CSIRT Network; and creating a critical alert system for the Mexican federal government.
- **2027 — Consolidation Phase:** This stage will involve creating a National Cyber Range for training and capacity-building. The range would train public officials, critical infrastructure operators, and response teams through realistic red team/blue team exercises involving ransomware, advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and cyber crises. It could also serve as a regional platform for Latin America and the Caribbean.
- **2028 — Maturation:** The Plan will incorporate the use of artificial intelligence (AI) for cyber defense and the development of a regional Latin America response center.
- **2029 — Leadership:** The leadership phase aims to position Mexico as a regional cybersecurity provider for Latin America and the Caribbean by exporting services provided by the General Directorate of Cybersecurity (DGCiber, which is Mexico's federal body for cybersecurity governance that sits inside the ATDT), including consulting, specialized training, technology transfer, regulatory guidance, and large-scale incident response support.
- **2030 — Transformation and Projection:** The final phase will create the Cybersecurity Observatory of Public Federal Administration, a permanent research and strategic analysis center that will track cyber incidents, emerging threats, institutional maturity, global cybercrime and cyberconflict trends, and new technologies, while producing evidence-based policy recommendations to guide Mexico's cybersecurity regulations, investments, and capacity-building efforts.

At the time of this writing, public reporting indicates that the activities identified in the Foundation Phase of 2025 have been completed. However, Insikt Group has been unable to find sufficient publicly available sources to verify progress on key components of the Expansion Phase in 2026. For instance, while Senator Jesús Lucía Trasviña Waldenrath of the ruling MORENA party presented a bill promoting cybersecurity coordination in January 2026, it is unclear if this proposal is related to the General Cybersecurity Law outlined in the Plan. It has not been voted on, and Insikt Group has not identified any other legislative proposals as of this writing. Similarly, Insikt Group is unable to determine whether a proposed broad-based cyber education campaign targeting federal employees ("APF Cibersegura," meant to be launched in the second quarter of 2026) or a planned creation of an online platform for a virtual training academy for government employees (meant to be operational in the second quarter of 2026) has been implemented as planned.

The timing of the Plan is significant given Mexico's currently heightened international visibility and exposure. The 2026 FIFA World Cup, which began on June 11, 2026, and is being hosted across Canada, Mexico, and the US, will place Mexico's digital infrastructure, public services, transport systems, telecommunications networks, ticketing platforms, hospitality sector, and local government systems under unusual strain and scrutiny. Mexico's three host cities — Mexico City, Guadalajara, and Monterrey — will be focal points for international visitors, media coverage, commercial activity, and public security operations, making them attractive targets for cybercriminals, hacktivists, and potentially state-sponsored actors seeking disruption, financial gain, or reputational impact. As Insikt Group has shown in previous research around major sporting events such as the 2024 Paris Olympics and the 2022 FIFA World Cup in Qatar, mass gatherings like these are likely targets for cybercriminals targeting critical sectors with ransomware, hacktivists aiming to disrupt due to geopolitical conflicts, state-sponsored actors engaging in espionage and influence operations, and physical safety threats from criminal organizations and extremist groups. During the 2024 Olympics, Insikt Group identified multiple instances of the Chinese state-sponsored group RedLima engaging in opportunistic cyber-espionage operations against select attendees or Olympic-affiliated organizations.

This Plan builds on years of Mexican efforts to flesh out the country's cybersecurity policy. Mexico published a National Cybersecurity Strategy in 2017, and while some critics suggested it prioritized digital rights over addressing cyber threats and lacked clarity and institutional coordination, it was widely hailed as a step in the right direction. Still, because it was issued at the end of the 2012–2018 administration of former President Enrique Peña Nieto, its implementation was essentially overtaken by the 2017 presidential election. Peña Nieto's successor, Andrés Manuel López Obrador, largely deprioritized cyber policy during his six-year administration — and the issue lay dormant until the current president, Claudia Sheinbaum, took office in 2024.

As a result, Mexico entered the Sheinbaum administration without a comprehensive national cybersecurity strategy, despite having a national incident-response body in CERT-MX, a national CERT responsible for helping prevent, mitigate, and respond to cyber threats affecting institutions in Mexico and hosted by the National Guard. In addition, Mexico has military CSIRTs, including the incident-response team associated with the National Defense Secretariat (SEDENA-CSIRT) and CSIRT-SEMAR, the Navy's incident-response team. These are sectoral teams focused on identifying, managing, and responding to cyber incidents within Mexico's defense and military ecosystem. With the announcement of the Plan, Mexico aims to incentivize stronger coordination and common standards and to create a single, unified civilian mechanism to support federal agencies.

Threat Analysis

The proposed National Cybersecurity Plan identifies three primary cybersecurity threats to Mexico: organized crime, geopolitical threats, and emerging AI threats. The Plan acknowledges the threats posed by cyber threat actors and state-sponsored groups, industrial and governmental espionage, targeting of critical infrastructure, disinformation campaigns during elections, hacktivism, and the widespread accessibility of AI, which cybercriminals can leverage to advance schemes such as phishing and deepfakes for fraud, automation and escalation of attacks, and evasion of detection and security controls. Insikt Group conducted further research into Mexico's cyber threat landscape since 2020, which supports these findings and provides additional insights. We believe the cybercriminal threat landscape has been defined by six persistent trends: state-sponsored activity, ransomware, financial malware and fraud, data breaches and theft, hacktivism, and organized crime and money laundering. Most of the cyber incidents impacting Mexico appear to be driven by financial motives. Mexico is among the top targeted countries in Latin America and has the second-largest economy in the region. The government, healthcare, and financial sectors have been heavily exposed. This decade has been marked by a steady increase in the frequency of attacks, broader victimology, and growing operational impact. Mexico’s proposed cybersecurity plan outlines explicit measures to prepare for ransomware, which is the primary threat we identified.

Ransomware, financial malware, and the sale of dark web data illustrate ongoing cyber risks. Mexico’s public sector has routinely been targeted, likely due to over-reliance on legacy systems, insufficient cyber maturity, and the concentration of valuable, often sensitive data such as personally identifiable information (PII). Insikt Group has observed numerous references to compromises affecting Mexican state governments, municipalities, civil registries, and public utilities. The financial sector faces unique risks at several levels, as threat actors have targeted both enterprises and consumers directly to gain initial access. Mexico has also experienced geopolitically charged cyber intrusions and hacktivism-driven document leaks.

Threat actors are opportunistic, often seeking to exploit technical, psychological, and organizational weaknesses. During times of social and political tension, attention becomes fragmented, and balancing workloads becomes difficult; security vigilance may suffer as a result. Security teams may become overloaded or be redirected, potentially creating gaps in detection. The teams’ emotions may also be heightened, enabling threat actors to exploit the looming sense of urgency and increasing demand for information. Threat actors may plan targeted cyberattacks during public crises because operational disruptions or delays may be mistaken for unrest-related effects, making attribution harder and allowing them to blend in.

Given that the 2017 National Cybersecurity Strategy was never realized and no updates on its implementation were ever provided, this proposed National Cybersecurity Plan has already made more significant strides toward its vision's execution.

State-Sponsored Activities

Insikt Group assesses that Mexico is an attractive target for state-sponsored cyber activity because of its deep integration with US supply chains, nearshoring-linked manufacturing base, and underdeveloped cyber governance. There have been multiple cases of state-sponsored activity affecting organizations in Mexico in recent years, including some Chinese state-sponsored activity likely aimed at acquiring valuable telecommunications research data and intellectual property. In February 2025, Insikt Group revealed that TAG-141 (FamousSparrow) had deployed SparrowDoor malware against Mexico's Universidad Nacional Autónoma, likely as part of a campaign to access research in areas related to telecommunications, engineering, and technology. Insikt Group has found additional instances of TAG-141 targeting research institutes dating back to 2022. Additionally, Asia-linked TGR-STA-1030 was observed targeting at least 70 government and critical infrastructure organizations to conduct cyberespionage, and two of Mexico's ministries were reportedly compromised, likely due to international trade announcements. Mexico has also been subjected to North Korea-sponsored remote IT-worker schemes, and in January 2025, a Mexican national was indicted for facilitating a scheme that targeted multiple US and European companies in order to generate revenue for North Korea.

Ultimately, while the National Cybersecurity Plan recognizes that geopolitical tensions raise the risk of government and corporate cyber espionage, it does not provide further details on specific plans to address foreign-state-linked cyber threats beyond emphasizing the need for federal and state coordination, critical infrastructure protection, and incident response.

Ransomware

Insikt Group assesses that ransomware is the dominant threat to organizations operating in Mexico. Ransomware attacks impose significant financial burdens on businesses, ranging from ransom payments and remediation costs to reputational and brand damage, possibly even resulting in the loss of customers. The ATDT reported that Mexico has the second-most ransomware victims documented in Latin America (after Brazil), having identified 155 victims from November 2019 to September 2025, of which sixteen incidents were disclosed by official sources and five by unofficial sources. According to the Plan, sources of cybersecurity breaches include official communications, press conferences, and public reports from Banxico (Mexico's Central Bank). However, the Plan does not mention victims of ransomware groups that have been dismantled by international law enforcement (such as Maze, Conti, and Hive).

From January 2020 until April 2026, Insikt Group identified and documented 223 ransomware incidents involving 64 ransomware groups and over 100 victims across Mexico. The data collected in our victimology table contains all publicly known ransomware victims listed on the associated ransomware blogs. The top ransomware groups that impacted Mexican entities this decade are LockBit Gang (BITWISE SPIDER, DEV-0396, Flighty Scorpius), Qilin (Agenda), CL0P (FANCYCAT), Kazu, and ALPHV

(BlackCat), as demonstrated in **Figure 1**. The top industries affected were government, manufacturing, information technology, and food and beverage, as demonstrated in **Figure 2**.

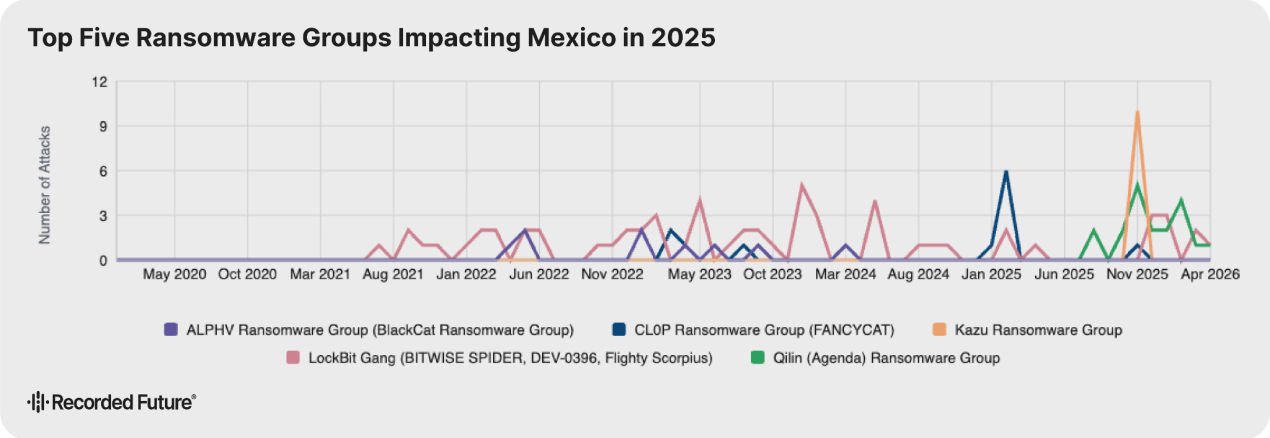

Figure 1: *Top five ransomware groups impacting Mexico in 2025 (Source: Recorded Future)*

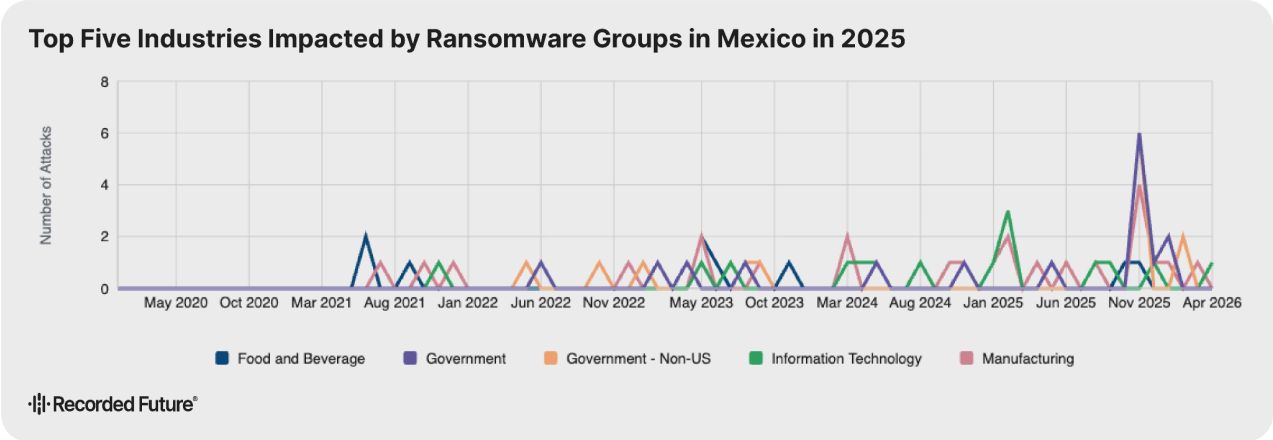

Figure 2: *Top five industries impacted by ransomware groups in Mexico in 2025 (Source: Recorded Future)*

Widespread ransomware campaigns heavily impacted government infrastructure and other essential service providers. LockBit was the clear leader, having conducted the most ransomware attacks against entities in Mexico, totaling 61. However, in early 2024, LockBit operators and infrastructure were disrupted by the US, the UK, and other international law enforcement in Operation Cronos.

In March 2026, the Institute for Security and Technology (IST), a US-based think tank, launched the México Ransomware Task Force to address the rising ransomware threat to Mexico's critical infrastructure and digital economy. This aligns with many of the goals outlined in the proposed Plan by prioritizing ransomware monitoring and mitigation. The four pillars of the México Ransomware Task Force are: Deter, Disrupt, Prepare, and Respond.

Financial Malware and Fraud

Insikt Group found that financial malware and fraud remain prominent issues in Mexico. Although the Plan does not explicitly provide direct solutions to mitigate this growing threat, it does acknowledge the rise of AI deepfakes and the importance of increased investment in cybersecurity solutions and talent. The Plan recognizes that the 2026 FIFA World Cup is a major international event and that Mexico should therefore guarantee the digital security of critical infrastructure, essential services, financial systems, online platforms, and other technological assets associated with its hosting. The Plan also proposes several projects to advance human capacity development and cybersecurity culture, including the introduction of a National Cybersecurity Awareness Campaign aimed at the general public to inform them about everyday risks such as phishing, social engineering, and deepfakes, and to educate them on data protection on social media and the secure use of digital financial services.

Based on findings from Insikt Group's "2025 Year in Review: Malicious Infrastructure" report, Mexico was among the top five countries with the most victims of infostealers. In 2025, AsyncRAT, DanaBot, and KV-Botnet were the top three malware families, respectively, based on the number of unique victims, and DanaBot, Beavertail, and LummaC2 led in observed infections in Mexico. Mexico was also among the top five largest issuer countries for stolen cards on the dark web in Latin America, with approximately 162,000 records in the first quarter of 2026. In 2025, Mexico had approximately 780,000 payment cards exposed on the dark web. Insikt Group assesses that this may be due to Mexico's large population and its position as the region's second-largest economy, making it a desirable target.

Active since 2022, the Fenix botnet began targeting users of government services, particularly tax-paying individuals in Mexico in 2024. Insikt Group found that the botnet often exploits tax season by impersonating official government portals such as the Tax Administration Service (SAT) and the Internal Taxes Service (SII). The Fenix botnet infrastructure includes two layers: Tier 1 for payload delivery, C2, and hosting control panels; and Tier 2, a "Central Server" likely for data collection and management. The operators leverage regional expertise and likely collaborate with the broader cybercriminal ecosystem (ransomware affiliates, for instance) to sell initial access for profit.

Insikt Group has observed persistent, financially motivated malware operations targeting the banking sector, fintech platforms, and individual consumers in Mexico. Among the most prolific banking trojans active over the past few years are Mispadu, Grandoreiro, and Casabaneiro (Mekotio). In 2024, a variant of the Mispadu Stealer targeted financial and cryptocurrency institutions in Mexico. Grandoreiro has been observed targeting victims in Mexico since at least 2020, during the onset of the global COVID-19 pandemic. In 2022, a Grandoreiro variant was observed leveraging enhanced detection evasion techniques and had several new features: keylogging, automatically applying updates to itself, web injection, command execution, manipulation of desktop windows, luring victims to otherwise malicious URLs, imitating mouse or keyboard movements, and generation of C2 domains via a domain generation algorithm (DGA). In that particular campaign, the phishing lures impersonated government officials or referenced mortgage loans. In 2024, Casabaneiro (Mekotio) was observed targeting financial systems in several Latin American countries, including Mexico, demonstrating the ability to produce fake

banking pop-ups to capture banking credentials, capture screenshots, log keystrokes, and access clipboard data.

Data Breaches and Theft

The Plan highlights the threat that data breaches and theft pose to Mexico, with a particular focus on ransomware group activity. However, many individual threat actors compromise systems and sell breached data without relying on ransomware or extortion tactics. These data breaches are often circulated, recycled, and resold for profit.

Leveraging the Recorded Future Intelligence Operations Platform, Insikt Group found nearly 500 references to posts on dark web special-access forums when Mexico was deemed the target of a cyberattack between January 2020 and April 2026. These references span 26 industries and 308 unique usernames. The most popular dark web special-access forums used by threat actors targeting entities in Mexico were DarkForums, followed by BreachForums 2, Altenen Forum, Leakbase Forum (Seized), and T00ls Forum. These are considered low-tier forums as they are easily accessible and commonly used to leak and sell stolen data.

Mexico has experienced instances of high-profile data leaks in recent years. In 2024, data from the presidential press system belonging to over 300 journalists was leaked (1, 2, 3). In February 2026, the National Commission of Insurance and Surety (CNSF) publicly disclosed via an official notice that an unknown threat actor gained unauthorized access, resulting in the exposure of intermediary ID credentials. Using the Recorded Future Intelligence Operations Platform, Insikt Group identified a dark web reference on DarkForums from the threat actor “adrxx” claiming to have leaked this data. In 2025, the threat actor “Mexicnon” auctioned 23,000 Mexico-issued payment cards on the top-tier Exploit Forum.

Hacktivism

Mexico’s geographical location between the US and the rest of Latin America exposes it to unique geopolitical risk. The threats identified by the Plan include governmental and industrial espionage, attacks on critical infrastructure, disinformation and misinformation campaigns during elections, and hacktivism with political motives.

Insikt Group has identified hacktivist trends impacting Mexico in recent years. The hacktivist group Chronus Team emerged in late 2025, primarily targeting institutions in Latin America, particularly Mexico, Argentina, Brazil, and Bolivia. As of early 2026, the hacktivist group has claimed responsibility for significant data leaks affecting public organizations across the education, insurance, law enforcement, healthcare, and government sectors in Mexico. Its modus operandi includes web defacements, data leaks via Telegram channels, and loosely affiliating with other hacktivist and criminal groups to gain attention and increase its reputation. The group’s targeting method is also driven to garner media attention, which can oversensationalize its capabilities, resulting in the spread of fear, uncertainty, and doubt (FUD). Chronus Team claims it wants to expose security vulnerabilities while

demonstrating financial motivations through exclusive data sales and offerings. The group underwent structural changes in March 2026 by merging with Mexican Mafia Team to form "Chronus Mafia," reflecting an expansion of its operational scope. Common tactics include social engineering, phishing, and exploiting weak security protocols across sectors. Overall, Chronus Team's operations reflect a blend of hacktivism with financially motivated cybercrime within a rapidly evolving landscape of Latin American cyber threats. Another hacktivist group, Guacamaya, compromised Mexico's Secretariat of National Defense in 2022, as noted above. That group decided on targets based on whether it believed they contribute to environmental decline and the repression of indigenous populations in Latin America.

Organized Crime and Money Laundering

The Plan identified organized cybercrime as a significant threat to Mexican cybersecurity. While acknowledging the new role that the National Guard plays in combating this threat, the Plan proposes the creation of a CSOC (National Cybersecurity Operations Center [SOC]) and the National APF CSIRT (CSIRT-APF) as dedicated civil solutions to prevent, detect, analyze, and respond to incidents that affect federal institutions. While the Mexican DTOs are not explicitly referenced in the Plan, we assess that DTO members have and will continue to rely on cybercrime-as-a-service to surveil, intimidate, and even kill informants who have been found cooperating with law enforcement.

Capital flight restrictions in China have also created an opportunity that CMLNs and Mexican DTOs have learned to exploit. In 2024, TRM Labs reported that a notorious Sinaloa Cartel affiliate used cryptocurrency to launder drug proceeds. The US government-led Operation Fortune Runner has resulted in the indictments and arrests of numerous participants in this criminal activity.

Figure 3: *Steps outlining the global fentanyl supply chain that highlight how illicit drugs are ultimately laundered (Source: Drug Enforcement Administration)*

Mexican DTOs have been proven to leverage CMLNs to clean their illicit drug proceeds. As a result, Chinese money brokers have a long-established presence in regions controlled by transnational criminal organizations such as the Sinaloa Cartel and the Cártel de Jalisco Nueva Generación (CJNG), facilitating money laundering for both groups. CMLNs use a trade-based system in which associates in China buy high-value goods (such as electronics, jewelry, and clothing), send them to Mexico, and sell them to generate legitimate proceeds in local pesos for the DTOs. This method rose in popularity following Mexico's 2010 anti-money laundering (AML) rules, which set limits on USD cash deposits, leading DTOs to rely on the informal economy established by the Chinese underground banking system (CUBS), thereby increasing dependence on these CLMNs.

Mitigations

Mexico's National Cybersecurity Plan provides an important foundation for strengthening the country's cyber resilience. As Mexico looks to emerge as a regional cybersecurity hub, and with the country currently co-hosting the 2026 FIFA World Cup in three cities, the Plan's strategic vision could potentially benefit organizations operating in Mexico by providing new tools that federal agencies, critical infrastructure operators, state and municipal governments, private-sector organizations, and individuals can use to reduce cyber risk. However, it is clear that Mexico faces particular threats in the form of state-sponsored activities, ransomware, financial malware, data breaches, hacktivism, and organized crime. With both the possible opportunities and threats in mind, Insikt Group recommends that organizations operating in Mexico consider the following mitigation measures:

- **Customers can leverage the Recorded Future® Intelligence Operations Platform.** As noted above, Insikt Group has identified additional ransomware incidents and possible victims beyond those cited in Mexico's National Cybersecurity Plan. Mexican organizations operating in high-risk sectors such as government, finance, energy, telecommunications, or critical infrastructure should consider using the Recorded Future platform to track threat actor activity, exposed credentials, vulnerability exploitation, dark web chatter, brand impersonation, and risks to internet-facing assets.
- **Adopt cybersecurity best practices.** Organizations operating in Mexico seeking to improve their cyber posture should consider adopting international standards to get ahead of upcoming policy shifts. Although the Plan does not mention mandatory adoption of cyber standards, such a mandate could be included in the upcoming Cybersecurity Law. Chile's cybersecurity framework, for example, creates domestic regulatory obligations to structure information security management, planning, and incident response. Organizations operating in Mexico could, in anticipation of heightened cyber standards, transition to making the implementation of frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or ISO/IEC 27001 compulsory, thereby establishing minimum cybersecurity baselines. NIST offers practical guidance for identifying, protecting against, detecting, responding to, and recovering from cyber threats, while ISO/IEC 27001 provides an internationally recognized standard for building and certifying an information security management system.
- **Conduct cybersecurity scenario planning exercises, promoting interactive and simulated exercises to help improve incident response plans.** Organizations in Mexico should consider improving their cyber posture by preparing for plausible scenarios such as ransomware attacks, data breaches, cyber espionage, hacktivism, and other digital threats, and engaging in cybersecurity wargaming and practical exercises to improve readiness. These exercises would help test not only technical response, but also leadership decision-making, public communication, legal coordination, and cross-border information sharing.
- **Educate employees and the general public.** Mexican decision-makers, in coordination with leading organizations in cyberspace, may want to consider the Plan as a way to raise public

awareness and improve cyber hygiene across society. A national campaign could explain how individuals, schools, small businesses, and local governments can report cyber incidents, recognize phishing, protect accounts with multifactor authentication, avoid credential reuse, back up important data, and respond to ransomware or fraud. By improving public awareness, Mexican decision-makers can reduce the number of cyber incidents while also increasing trust in official reporting channels.

Outlook

The 2026 FIFA World Cup will be an early test of Mexico's cyber resilience and will likely inform the implementation of the National Cybersecurity Plan. Mexico is hosting matches in Mexico City, Guadalajara, and Monterrey, placing government systems, airports, stadium operations, transportation networks, hotels, telecommunications providers, payment systems, and public-facing digital services under heightened scrutiny. Cyber risk around the tournament is likely to be elevated, as the event creates a target-rich environment for ransomware groups, hacktivists, fraud actors, credential thieves, and disinformation networks seeking financial gain or disruption (see Insikt Group's 2026 FIFA World Cup threat assessment here). If a cyber incident occurs, it will likely shape public debate over cybersecurity in Mexico and attract greater international attention to any perceived gaps.

This is significant, as in the coming months, Mexico will very likely move from the planning stage to the implementation of its Plan. While the Plan provides a blueprint for greater cyber coordination, its implementation will depend in large part on the proposed Federal Cybersecurity Law, set to be presented in 2026 by the ruling National Regeneration Movement (MORENA) party, which, along with its allies, holds a controlling majority in Congress. According to the Plan, the law will define legal obligations, institutional authorities, and regulatory mechanisms needed to enforce the vision outlined in the Plan. As the legislative process advances, the debate will likely focus on the powers of national cybersecurity authorities, privacy concerns, private-sector compliance obligations, and data protection implications. Even if the law is passed in 2026, implementation will likely unfold gradually over several years — as the Plan makes clear — as Mexican agencies like the ATDT issue more detailed regulations and build out the institutional frameworks needed to ensure compliance.

Looking further ahead, Mexico's cyber risk environment will likely come under even greater international scrutiny amid deeper security cooperation between the US and Mexico. In recent years, Washington has sought to broaden its coordination on security issues with its Mexican counterparts, with a particular focus on combating organized crime and illicit drug trafficking. However, cyber concerns have also become an important part of these ongoing security conversations, and led to the creation of a US-Mexico Working Group on Cyber Issues in 2022. As the two countries explore ways to cooperate on security policy, cybersecurity will almost certainly continue to grow in prominence as a central pillar of the bilateral relationship. Mexico's ability to implement the Plan and build cyber resilience will shape not only its domestic cyber posture but also its credibility as a security, trade, and technology partner for the US.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com