Duke SANFORD | CYBER POLICY PROGRAM

Securing the Backbone: Enhancing Cyber Resilience in Latin American SMEs to Safeguard Critical Infrastructure and U.S. Supply Chains

Isabella Delgado and Ana Martinez[1]

[1] This paper was written while the authors were Duke University students and Summer Interns at the Center for Latin American Convergence (CCLatam). The authors would like to thank Andy Kotz for his assistance with the paper.

Executive Summary

Significant new economic opportunities have been presented to Latin America (LATAM) due to the technological decoupling of the United States (U.S.) and China, particularly in the semiconductor industry. The growing strategic distrust between these two global powers has led to a shift in supply chain dynamics, offering LATAM countries a chance to capitalize on nearshoring and friend-shoring initiatives. The U.S. government's increased technological restrictions and support for domestic industries have allowed LATAM countries to integrate into critical global semiconductor supply chain segments.

Small and medium-sized enterprises (SMEs) in Latin America yet have a critical role in supporting national infrastructure yet face cybersecurity challenges that threaten their operability. Despite being vital to the economy and job creation, SMEs are particularly vulnerable to cyberattacks due to limited resources. Recent ransomware attacks in Colombia, Costa Rica, and Chile highlight the devastating impacts of cybersecurity breaches on essential services and national security. The paper advocates for implementing advanced cybersecurity technologies like Extended Detection and Response (XDR). It proposes initiatives for LATAM governments to enhance cybersecurity resilience through regional cooperation, educational programs, and leveraging international development funding.

Strengthening LATAM's cybersecurity infrastructure to protect critical sectors and foster economic collaboration within the region and with global partners is increasingly important. By adopting proactive cybersecurity measures and leveraging economic opportunities from the U.S.-China supply chain decoupling, LATAM countries can enhance their strategic importance in the global economy while ensuring the stability and security of their digital ecosystems.

Introduction

Currently, there are opportunities for portions of the semiconductor value chain to move to Latin America to avoid supply chain disruptions.[2] Doing so will require cost-effective, reliable water and power in LATAM countries. Critical

[2] https://www.nytimes.com/2024/04/01/opinion/intel-costa-rica-semiconductors.html

infrastructure like water and power relies upon various small and medium-sized suppliers who support the delivery of utilities in these countries.[3] However, these suppliers likely need more resources to invest in leading-edge cybersecurity tools. Subsequently, this lack of investment creates the risk of ransomware attacks by politically motivated organizations that in turn will negatively impact the U.S. due to disruptions to the reorganized semiconductor supply chain.

Consider a scenario in which the United States has decoupled from China and now relies on near-shoring to Latin American countries for the integrity of crucial supply chains. This dynamic of reorganized supply chains would benefit the U.S. by lessening its dependence on China. Nonetheless, the emergence of reorganized supply chains creates new vulnerabilities for the U.S. as it would confront the second-order negative impacts of ransomware attacks on its suppliers in Latin America.

One can imagine a Latin American country making the politically contentious decision to recognize Taiwan and, in doing so, aggravating the Chinese government. This Latin American country now fears that the Chinese government may pursue ransomware as retribution. This concerns the U.S. because, under reorganized supply chains, the potential for disruption to their supply of components or materials increases. For example, the U.S. relies on Asia for semiconductor testing equipment and advanced semiconductor packaging supplies, such as chip carriers and cover tape.[4] Under reorganized supply chains, the production of these items could feasibly be moved to Latin America if there was a sufficient guarantee of sales to mitigate the start-up costs.[5]

The economic opportunities in the LATAM region require reliable and secure critical infrastructure (CI). These CI services depend upon an ecosystem of local service vendors and suppliers, often small and medium businesses. Ransomware attacks from the Chinese government or government-supported organizations targeted towards these SMEs could put business continuity at risk. Consequently, because large CI enterprises in Latin America are only as secure as their small and medium vendors, it would be in the best interest of the U.S. and countries in the LATAM region to participate in a model that strengthens the cybersecurity resilience of these small and medium CI vendors.

Background

[3] https://www.csis.org/analysis/catalysts-change-how-entrepreneurs-are-transforming-latin-america
[4] https://www.wsj.com/tech/asias-chip-giants-hustle-to-maintain-their-edge-over-the-u-s-2edd6904
[5] Ibid.

Decoupling the US-China supply chain provides LATAM with an economic opportunity to fill the void (nearshoring/friend-shoring).

The U.S. and China have spent years becoming technologically interdependent within an expanding economic relationship. However, as these countries have begun to view one another with increasing suspicion, this technological interdependence has become a source of strategic vulnerability for both countries. Consequently, the technological decoupling of the U.S. and China is underway. As the Harvard Business Review articulated, China's primary "dual circulation" strategy involves three key objectives: eliminating dependence on foreign entities for critical technology and products, facilitating the domestic dominance of indigenous firms, and leveraging this dominance into global competitiveness.[6] Motivations for this decoupling from the American side include the U.S.'s fear of China exploiting the technological relationship for undesirable aims, including espionage, military modernization, and the spread of disinformation.[7] The state-supported Chinese cyber operation Volt Typhoon, which compromised thousands of internet-connected devices as part of a larger effort to infiltrate western CI using living-off-the-land techniques, demonstrates China's potential for espionage.[8] A report published by Microsoft indicates that Volt Typhoon has been active since mid-2021, targeting U.S. infrastructure in Guam and elsewhere.[9] The threat actor's intention to perform espionage and remain undetected for as long as possible highlights China's potential to exploit its technological relationship with the U.S. for undesirable aims.

Decoupling the US-China supply chain will inevitably affect global corporations' strategies. The profits of many high-tech companies in the U.S. may be affected once they cannot utilize the expansive Chinese market. China's market accounts for 50% of the global semiconductor demand. U.S. companies like Intel export billions of dollars worth of microchips to China.[10] However, this is quickly changing as the U.S. tightens export controls. U.S. export controls on advanced

---

[6] https://hbr.org/2021/05/the-strategic-challenges-of-decoupling#:~:text=Widely%20publicized%20tit%2Dfor%2Dtat,America's%20civil%20and%20military%20infrastructure

[7] https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

[8] https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer

[9] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[10] https://www.globaltimes.cn/page/202307/1294524.shtml?id=11

semiconductor technology enacted in October 2022 prohibit U.S. firms from exporting advanced semiconductor chips to China without a government-issued license.[11] This trend of restrictions has only continued; the U.S. government recently told Intel and Qualcomm that they would no longer be able to export some chips to the Chinese company Huawei.[12] Ongoing U.S. export controls and China's market-share goals for domestic firms can adversely affect U.S. tech companies' revenue if they cannot form relationships with new foreign firms.

Recently, the U.S. government has moved to impose increasing technological restrictions, including export controls, licensing denials, visa bans, sanctions, and tariffs.[13] Alongside these defensive policies, offensive actions taken by the U.S. include increased government support for research and development in key industries such as the semiconductor industry. The semiconductor industry represents a key industry as the interdependency of the global supply chain for semiconductors leaves the U.S. and China economically and strategically vulnerable. Reorganizing the semiconductor supply chain would require the U.S. to seize opportunities for near-shoring and friend-shoring in Latin American countries positioned to play a key role in certain parts of the semiconductor supply chain.

The semiconductor supply chain often requires multiple international supply lines to create just one chip. The stages of semiconductor production are each concentrated in a few regions of the world. For instance, a chip's design may be developed in the U.S., fabricated in Japan, assembled in another country in China, and tested back in the U.S.[14] The global nature of this supply chain, with different production stages concentrated in different regions, makes it susceptible to disruption. Today, the U.S., China, and the European Union confront significant vulnerabilities due to the offshoring of manufacturing capabilities and the global nature of high-tech manufacturing. The shortages in critical medical equipment and semiconductors necessary for constructing various electronic devices and automobiles in the U.S. following the COVID-19 pandemic highlighted the acute implications of such global supply chain interdependency.[15]

---

[11] https://www.csis.org/analysis/collateral-damage-domestic-impact-us-semiconductor-export-controls#:~:text=October%202022%3A%20The%20United%20States,than%2014%20nanometers%20(nm)

[12] https://asia.nikkei.com/Business/Tech/Semiconductors/U.S.-chip-equipment-makers-rely-on-China-for-40-of-sales

[13] https://www.csis.org/analysis/collateral-damage-domestic-impact-us-semiconductor-export-controls#:~:text=October%202022%3A%20The%20United%20States,than%2014%20nanometers%20(nm)

[14] https://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region

[15] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9350259/#:~:text=Most%20recently%2C%20the%20global%20shortage,demand%20when%20car%20production%20rebounded

As global powers move to decrease foreign technological dependence, the U.S. and Europe have indicated intentions to construct cutting-edge semiconductor fabs. To increase semiconductor supply chain resiliency and decrease reliance on global shipping companies, semiconductor companies in the U.S. have begun strides toward near-shore manufacturing activities. Many companies have looked toward countries in the LATAM region due to several factors, including its proximity and low-wage workforce.

The need to diversify supply chains prompted several governments to announce investments to foster semiconductor manufacturing. Europe announced its CHIPS Act in 2023 to encourage semiconductor production in the EU.[16] In 2022, the U.S. enacted the CHIPS and Science Act to boost American semiconductor research, development, and production.[17] Some government efforts have targeted countries in the LATAM region. In 2023, the U.S. State Department announced a new partnership with Costa Rica to explore semiconductor supply chain opportunities.[18] It announced a similar partnership with Mexico in March of 2024.[19] Other large companies, such as Micron and Qualcomm, announced additional investments in American semiconductor manufacturing. Part of Intel's IDM 2.0 Strategy to become a contending foundry services provider for the global semiconductor market includes $1.8 billion investment in Costa Rica. [20]

Actions Latin American Governments Can Take to Decrease Ransomware Attacks

Background on SMEs in Latin America

Small and medium-sized enterprises (SMEs) in Latin America have less than 100 employees, and SMEs play a pivotal role in Latin America's economic landscape.[21] These businesses comprise a staggering 99.5% of all businesses in the region and account for 60% of employment.[22] Despite their significant presence, they contribute only 20-25% of the gross domestic product (GDP) due to various financial and productivity constraints.[23] Their development is crucial for achieving

[16] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

[17] https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

[18] https://www.state.gov/new-partnership-with-costa-rica-to-explore-semiconductor-supply-chain-opportunities/

[19] https://www.state.gov/new-partnership-with-mexico-to-explore-semiconductor-supply-chain-opportunities/

[20] https://www.reuters.com/business/intel-invest-12-bln-costa-rica-over-next-two-years-2023-08-30/

[21] https://www.oecd.org/latin-america/regional-programme/productivity/sme-development/

[22] https://www.oecd.org/latin-america/regional-programme/

[23] Ibid.

broad-based and sustained economic growth, particularly as the region grapples with the effects of the pandemic and other global shocks.

SMEs are fundamental to job creation, especially regarding CI, and serve as key suppliers of goods and services to a large population segment, including the United States. In some countries within Latin America, SMEs make up over 80% of formal employment in the private sector.[24] However, their contributions to the economy and formal employment can vary significantly, with countries like Mexico and Chile seeing much lower proportions.

SMEs and Critical Infrastructure (CI)

Latin America's critical infrastructure, encompassing sectors such as energy, transportation, and healthcare, heavily relies on the cybersecurity resilience of SMEs. These sectors are integral to national security and economic stability, and any cybersecurity failure within an SME can have cascading effects throughout the broader digital ecosystem. Such failures can lead to significant financial and reputational losses and service disruptions.

Equally crucial, these SMEs are instrumental in supporting the region’s water and energy production and delivery. As the demand for clean energy and efficient water management grows, SMEs are increasingly being relied upon to implement the infrastructure necessary for these essential services. From the development of electric vehicles and biofuels to the deployment of advanced energy management systems in water utilities, these small and medium-sized enterprises are at the forefront of addressing Latin America's environmental and technological challenges.[25] For instance, SMEs have been pivotal in projects like the Alagoas Water and Sanitation Company's efforts to improve water access in Brazil or the integrated energy management program by Empresas Públicas de Medellín in Colombia, which has significantly enhanced the efficiency and reliability of water systems.[26]

Given their role in supporting critical infrastructure, SMEs must prioritize robust cybersecurity measures. However, many SMEs need more resources to implement comprehensive cybersecurity programs, making them particularly vulnerable to

[24]https://www.undp.org/latin-america/blog/graph-for-thought/small-businesses-big-impacts-supporting-productive-smes-engine-recovery-lac
[25] https://www.csis.org/analysis/catalysts-change-how-entrepreneurs-are-transforming-latin-america
[26] https://www.worldbank.org/en/news/feature/2013/09/03/latin-america-water-loss-energy-efficiency

cyberattacks. Common attack vectors include malware, phishing, and business email compromise (BEC).[27]

Cybersecurity Vulnerabilities and Risks

SMEs in Latin America face numerous cybersecurity challenges. Their limited financial and technical resources hinder the ability to establish strong cyber defenses, making SMEs attractive targets for cybercriminals. The ripple effect of ransomware attacks can disrupt the SMEs, larger organizations, and CI sectors they support. In 2022, there were up to four times more cyberattacks for SMEs in Latin America, with attacks in Mexico increasing from 123,640 in 2021 to 323,434 in 2022; Brazil from 88,432 to 215,580 attacks; and Colombia from 39,627 to 161,589 attacks, respectively.[28] The following case studies from Colombia, Costa Rica, and Chile illustrate how ransomware attacks on SMEs and critical sectors can disrupt essential services and impact national security:

Colombia (2022; 2023)

In December 2022, a ransomware attack on Keralty, a major healthcare provider, severely impacted Colombia's healthcare system. The ransomware group RansomHouse breached Keralty's networks and compromised sensitive health data, including names, addresses, social security numbers, and medical records.[29] This breach led to significant disruptions in hospital scheduling systems, resulting in longer patient wait times and loss of access to essential services.[30]

In September 2023, another ransomware attack targeted one of Colombia's internet service providers, IFX Networks.[31] This attack affected 78 state entities and 762 private companies, including the Ministry of Health and Social Protection, the judiciary branch, and the Superintendency of Industry and Commerce.[32] The incident paralyzed the operations of the Colombian government, with two million scheduled legal proceedings suspended for seven days due to frozen judicial web

[27]https://www.forbes.com/sites/forbestechcouncil/2022/04/08/critical-infrastructure-attacks-and-lessons-for-smbs/
[28]https://www.ventasdeseguridad.com/en/2022071122263/news/enterprises/smes-in-latin-america-up-to-four-times-more-cyberattacks-in-2022.html
[29]https://www.kiuwan.com/blog/latam-data-breaches-top-3-countries-affected/#:~:text=The%20three%20countries%20that%20reported,Chile%2C%20Mexico%2C%20and%20Colombia.
[30] Ibid
[31]https://www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-cyberattack-petro-2023-09-18/#:~:text=Sept%2018%20(Reuters)%20%2D%20More,told%20journalists%20in%20New%20York
[32]https://thomasmurray.com/insights/colombia-fights-back-devastating-ransomware-attack#:~:text=The%20Colombian%20government%20alleges%20that,take%20legal%20action%20against%20IFX

portals.[33] Many health centers also lost online services, preventing patients from making appointments or obtaining prescriptions as doctors could not access medical records.

Case Study: Costa Rica (2022)

In April 2022, Costa Rica experienced a major ransomware attack by the Russia-based group Conti, marking the fifth-largest global cyberattack.[34] Conti demanded $10 million to prevent the leak of sensitive data from the Ministry of Finance, including citizen tax records.[35] The attack shut down critical tax filing systems and brought economic effects. A subsequent attack by the Hive group in May 2022 targeted the Social Security Agency (CCSS), disrupting medical systems and leading to the cancellation of over 158,000 medical procedures.[36] These attacks on local data centers and private cloud systems forced many government functions, such as the public medical and tax collection systems, to revert to manual documentation.[37]

Costa Rica did not pay the ransom, but the attacks led to significant economic and operational disruptions. The government declared a national emergency, allocating roughly $24 million for response operations.[38] The cost of the rehabilitation phase for CCSS alone exceeded $18 million.[39] Despite these efforts, the infrastructure was only partially repaired months after the attacks, affecting thousands of citizens. The lack of a national cybersecurity law, limited progress on a data-protection bill, and constrained CSIRT resourcing exacerbated the vulnerability. Costa Rica's position in the Global Cybersecurity Index deteriorated significantly, highlighting the urgent need for deterrence measures, especially for SMEs.

Case Study: Chile (2023)

Chile's increasing digitalization has brought significant cybersecurity risks. In May 2023, the Chilean Army suffered a ransomware attack by the group Rhysida, which affected internal networks and led to a data breach.[40] The attack caused intermittent unavailability of the army's websites, and Rhysida published 30% of

[33] Ibid.
[34] http://apnews.com/article/russia-ukraine-technology-business-gangs-costarica-9b2fe3c5a1fba7aa7010eade96a086ea
[35] https://osinter.dk/news/search?sort_by=publish_date&highlight=true&search_term=rican
[36] https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)#cite_note-8
[37] Ibid
[38] https://www.researchgate.net/publication/366719503_Ransomware_and_Costa_Rica's_national_emergency_A_defense_framework_and_teaching_case
[39] Ibid
[40] http://www.cronup.com/ejercito-de-chile-es-atacado-por-la-nueva-banda-de-ransomware-rhysida/

the stolen data.[41] Although an arrest was made, the root cause of the attack remains unclear. In addition, in October 2023, the ransomware group Black Basta targeted Chile's National Customs Service, infecting part of its digital infrastructure.[42] The Ministry of Interior and Public Security's CSIRT issued a warning and took preventive measures to ensure customs operations were not disrupted.[43]

XDR and Tools to Reduce Ransomware

The digital landscape has experienced a rapid increase in cyber threats, driving cybersecurity professionals to develop innovative defensive strategies for businesses. Among the most significant advancements is extended detection and response (XDR), which was introduced in 2018.[44] XDR, an evolution of endpoint detection and response (EDR), marks a shift in cybersecurity by offering an integrated approach to threat detection, response, and mitigation.[45] Traditional cybersecurity solutions have struggled with the complexity of modern ransomware attacks. By aggregating and correlating data from various sources within an organization's IT ecosystem—including endpoints, networks, cloud environments, and applications—XDR provides security teams with comprehensive visibility into potential threats and their broader context.[46] This contextual understanding enables the accurate identification of sophisticated, multistage attacks that might otherwise go unnoticed, significantly reducing the time between threat identification and mitigation.[47]

XDR vs. Traditional Ransomware Solutions

Extended detection and response (XDR) significantly advance traditional security solutions. Conventional approaches often operate in silos, concentrating on specific layers of defense such as endpoints, networks, or application security.[48] This fragmentation hinders their ability to effectively detect and respond to coordinated multivector attacks. In contrast, XDR integrates data from multiple sources,

---

[41]http://www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/

[42] http://www.csirt/gob.cl/noticias/10cnd23-00112-01/

[43]https://www.aduana.cl/superada-alerta-informatica-en-sistemas-de-aduanas/aduana/2023-11-10/140942.html.

[44]https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR#:~:text=Coined%20by%20Palo%20Alto%20Networks,response%20across%20all%20data%20sources

[45] Ibid

[46]https://www.vmware.com/topics/glossary/content/xdr-extended-detection-and-response.html#:~:text=XDR%20performs%20automated%20analysis%20and,and%20delivery%20of%20malicious%20artifacts

[47] Ibid

[48]https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR#:~:text=Coined%20by%20Palo%20Alto%20Networks,response%20across%20all%20data%20sources

including endpoints, networks, cloud environments, and applications, providing a broader perspective on threats and enabling the correlation of data across multiple vectors.[49] This integration helps uncover complex attack patterns that might otherwise go undetected.

Traditional solutions often lack context, providing isolated alerts that require manual investigation and correlation to understand the full scope of an attack.[50] XDR offers contextual insights by analyzing data across different layers of the IT environment, helping security teams comprehend attackers' tactics, techniques, and procedures (TTPs) and enabling a more informed response.[51] Additionally, traditional solutions depend heavily on manual intervention for threat analysis, investigation, and response, which can delay the detection and mitigation of attacks. On the other hand, XDR employs automation and machine learning to identify and respond to threats swiftly.[52] Automated playbooks can execute predefined actions based on the severity of the threat, reducing response time and allowing security teams to focus on more strategic tasks.

There are currently upwards of 40 vendors offering XDR capabilities globally.[53] The following two XDR solutions, CrowdStrike Falcon and Expel, offer features suitable for SMEs:

Crowdstrike Falcon XDR[54]

Founded in 2011, CrowdStrike is a leader in advanced endpoint protection and threat intelligence, offering cloud-native security solutions on a global scale.[55] Their Falcon XDR solution, established in April 2023, is a robust extension of CrowdStrike's well-regarded Endpoint Detection and Response (EDR) capabilities.[56] Falcon XDR gathers telemetry from various tools, analyzes threats across multiple domains, and provides coordinated responses through a unified platform.[57] The service correlates events and telemetry from endpoints, cloud services, identity systems, and third-party tools to create a prioritized stream of

[49]https://www.microsoft.com/en-us/security/business/security-101/edr-vs-xdr
[50]https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR#:~:text=Coined%20by%20Palo%20Alto%20Networks,response%20across%20all%20data%20sources
[51] Ibid
[52]https://www.bluevoyant.com/knowledge-center/edr-vs-xdr
[53]https://www.spglobal.com/marketintelligence/en/documents/the-rise-of-extended-detection-and-response.pdf
[54] Crowdstrike employees participate in Duke University's cybersecurity education programs. Crowdstrike did not provide any funding for the creation of this paper.
[55]https://www.spglobal.com/marketintelligence/en/documents/the-rise-of-extended-detection-and-response.pdf
[56]https://www.crowdstrike.com/platform/
[57]Ibid

alerts.[58] The platform automatically detects threats and supports advanced investigations using MITRE ATT&CK mapping and visualization, helping teams to understand and respond to threats more effectively.[59] Falcon XDR also features powerful analytics, root cause analysis, containment of suspicious activities, and automated response workflows.[60] Designed to enhance CrowdStrike's EDR capabilities, Falcon XDR is ideal for existing EDR users looking to expand their solution and for organizations with many endpoints to protect.

Expel[61]

Expel helps businesses of all sizes minimize risk by leveraging technology and human expertise to swiftly interpret security signals and address issues.[62] Utilizing its security operations platform, Expel offers managed detection and response (MDR), remediation, phishing protection, vulnerability prioritization, and threat hunting.[63] Expel's Managed Detection and Response provides 24/7 decision support, seamlessly integrating with existing technologies across various attack surfaces to maximize tech investments.[64] The platform automates vendor alert analysis to filter out false positives. It enriches significant alerts with context, resolving them with an average alert-to-fix time of 22 minutes for critical issues.[65]

As a leading MDR provider, Expel enhances security, minimizes risk, augments existing programs, and delivers detection and automation through cloud-focused solutions. Their Expel Workbench, the company's security operations platform, integrates personnel, expertise, and technology, allowing businesses to concentrate on building trust with clients.[66] Regardless of whether an organization has a security operations center (SOC), Expel can enhance security by rapidly analyzing and resolving issues. Through AI-driven triage, businesses achieve accelerated detection and response that scales with growth. Additionally, Expel provides comprehensive services, including phishing protection, threat hunting, and vulnerability management, ensuring consistent excellence for all clients.[67]

---

[58] Ibid
[59] https://expertinsights.com/insights/the-top-xdr-solutions/
[60] Ibid
[61] Expel is a portfolio company of Paladin Capital Group, which is the founding partner for Duke University's Cybersecurity Leadership Program and Chief Information Security Officer certificate. Paladin Capital Group did not provide any funding for the creation of this paper.
[62] https://expel.com/about/
[63] Ibid
[64] https://expel.com/services/managed-detection-response/
[65] https://expel.com/why-expel/
[66] https://expel.com/security-operations-platform/
[67] Ibid

Shared Services Programs for SMEs

The following literature review highlights two shared service programs that support SMEs and other businesses in the United States and the United Kingdom. Analyzing these tools provides a framework to help shape recommendations for Latin American policymakers to create funding mechanisms and shared service programs to expand educational awareness about cyber threats and provide tools at a reduced cost to such SMEs.

United States

The National Security Agency (NSA) offers a suite of threat-informed cybersecurity solutions to companies with active Department of Defense (DoD) contracts in the United States.[68] Within the DoD's program are three services that aim to reduce the risk of network compromise and protect sensitive information. First, the Protective Domain Name System (PDNS) service blocks connections to malicious domains, having already blocked over 1 billion such attempts.[69] Second, the Attack Surface Management service identifies and prioritizes network vulnerabilities, providing tailored reports for remediation.[70] Finally, the Threat Intelligence Collaboration also allows for the secure sharing of threat intelligence between the NSA and enrolled companies, significantly disrupting nation-state cyber campaigns.[71] Through this, the NSA establishes a collaboration channel with cyber threat analysts to share non-public, DIB-specific threat intelligence and mitigate suspicious cyber activity.

The NSA's program has helped many businesses ward off cyber threats while learning more about how nation-states carry out cyberattacks. The PDNS service currently processes 70 million DNS queries a day.[72] According to statistics compiled by the Cybersecurity Directorate's DNS provider, the service has thus far blocked billions of malicious queries, including ransomware activity and known nation-state spear phishing, malware, and botnets. This integrated service model enables the NSA to better prepare for future threats. The CCC sends the NSA

[68]https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/
[69]https://www.nsa.gov/Portals/75/documents/Cybersecurity/CCC/DIB_Services_NOV2023.pdf?ver=Gbol8Ev8D30uHtV2yjH0Nw%3d%3d
[70]Ibid
[71]https://www.nsa.gov/Portals/75/documents/Cybersecurity/CCC/DIB_Services_NOV2023.pdf?ver=Gbol8Ev8D30uHtV2yjH0Nw%3d%3d
[72]https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3774721/small-defense-contractors-share-how-nsa-gives-them-a-boost/

custom analytics of DNS data that allow it to understand better how nation-states target the DIB.[73]

This NSA program highlights the importance of emphasizing cybersecurity resilience at the lowest levels of critical supply chains. Over 1,000 industry partners have signed up for the NSA's Cybersecurity Collaboration Center's (CCC) no-cost cybersecurity services. Participating companies range from small businesses that provide critical components to the nation's most sensitive systems to major service providers that can help protect billions of endpoints.[74] These companies acknowledge the benefits of the NSA's program for their bottom line and national security. Small businesses make up 70% of the Defense Industrial Base's supply chain and have access to sensitive DoD information.[75] Like LATAM SMEs, these small businesses often lack the technical expertise and/or resources to defend themselves against sophisticated nation-state threats. The NSA's program success is rooted in recognizing that these companies are an attractive target for adversaries wishing to steal U.S. intellectual property. The key role played by these small companies in the DIB's supply chain renders them inseparable from national security interests.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) also offers several support programs for SMEs.[76] For example, CISA's Protective DNS Resolver is a solution that uses government and commercial threat intelligence to prevent systems from connecting to suspected malicious domains and has blocked nearly 700 million connection attempts from federal agencies since 2022.[77] This service is now being expanded to critical infrastructure entities, including healthcare, water, and education sectors. In addition, CISA's Cybersecurity Shared Services Pilot program aims to scale these protections to more entities and improve their cybersecurity resilience.[78]

---

[73] Ibid

[74] https://media.defense.gov/2023/Dec/19/2003362479/-1/-1/0/NSA%202023%20Cybersecurity%20Year%20In%20Review.PDF

[75] Ibid

[76] https://www.cisa.gov/

[77] https://www.cisa.gov/resources-tools/services/protective-domain-name-system-resolver

[78] https://www.cisa.gov/news-events/news/piloting-new-ground-expanding-scalable-cybersecurity-services-protect-broader-critical

Furthermore, the U.S. Small Business Administration (SBA) has launched a Cybersecurity for Small Business Pilot Program, providing $6 million in funding to state entities to enhance SMEs' cybersecurity infrastructure.[79]

United Kingdom

The United Kingdom also provides SMEs with a network of opportunities and resources to protect their cybersecurity capabilities. Notably, the National Cyber Security Centre (NCSC) launched the "Share and Defend" capability in May 2024, designed to protect the public and businesses against cybercrime and cyber-enabled fraud.[80] This program partners with Internet Service Providers (ISPs) to filter malicious domains and URLs, preventing access to harmful content.[81] The program utilizes PDNS and Takedown data, a procedure for asking an ISP or search engine to remove or disable access to illegal, irrelevant or outdated information, as a filter to locate suspicious cybersecurity threats; these services work with hosting providers to remove malicious sites and infrastructure from the internet. The proactive approach leverages data sharing and industry collaboration to disrupt cybercriminal activities and enhance online safety for UK businesses and the public.[82]

The NCSC also provides several resources to assist SMEs, including an online tool to assess vulnerabilities, a “Cyber Aware” advice page, a free Cyber Action Plan for personalized security recommendations, and sector-specific support.[83] Additionally, the NCSC offers cybersecurity training to help SMEs understand critical security topics and implement protective measures.

Proposal

Internal Funding Initiatives (LATAM Governments)

To effectively combat ransomware attacks on SMEs in Latin America, governments must prioritize the implementation of advanced cybersecurity technologies like Extended Detection and Response (XDR). The following recommendations target the public sector, encouraging Latin American

[79]https://www.sba.gov/article/2023/08/14/us-small-business-administration-announces-new-cybersecurity-grant-recipients-2023
[80]https://www.ncsc.gov.uk/information/share-defend-capability
[81] Ibid
[82]Ibid
[83]https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

governments to support cybersecurity initiatives through collaborative and independent actions.

Creation of a Latin American Cybersecurity Coalition

Latin American countries interested in advancing cybersecurity, such as Costa Rica, the Dominican Republic, Mexico, Panama, and Paraguay, should establish an opt-in government coalition. This coalition would focus on promoting cybersecurity policies and distributing XDR tools to SMEs across the region. This coalition can foster cooperation among public and private cybersecurity stakeholders by drawing inspiration from successful models like the European Cyber Security Organization (ECSO).[84] For example, ECSO has worked alongside the European Commission and other investors to create a platform totaling at least 1 billion Euros over five years. This funding has helped promote investments in European cybersecurity start-ups and SMEs. Member countries can develop a robust cybersecurity ecosystem that supports SMEs and critical infrastructure by pooling resources and sharing expertise.

The coalition can learn from ECSO's experience by forming a new Public-Private Partnership (PPP), building off an existing one, and creating a cybersecurity investment and shared services platform. This platform could both co-invest in cybersecurity entrepreneurship in Latin America, and provide SMEs with access to cybersecurity tools like XDR solutions at negotiated lower rates. In this hypothetical, Latin American governments can build on existing partnerships and organizations like Costa Rica's Cybersecurity Cluster or the Organization of American States (OAS) to create a centralized organization targeting business cybersecurity initiatives. With a targeted funding goal, like ECSO's €1 billion investment over five years, the coalition can attract investments and support for cybersecurity startups and SMEs. This approach would be a crucial first step in ensuring that Latin American SMEs have access to the latest cybersecurity technologies and resources, significantly reducing their vulnerability to ransomware attacks.

National Initiatives for Cybersecurity Education and Funding

Individual Latin American governments could also provide educational and funding resources to SMEs, mirroring successful strategies from countries like the United States and the United Kingdom. These countries have demonstrated the importance of institutionalizing cybersecurity practices, launching educational and

[84] https://esco.ec.europa.eu/en

training initiatives, and fostering collaboration between corporate and nonprofit actors.

Similar to the U.S. NSA's Defense Industrial Base (DIB) Cybersecurity Program, which implements a three-part strategy to provide cybersecurity tools for SMEs, governments can create service programs that reduce network compromise risk and protect sensitive information. These programs can include intelligence systems that block connections to malicious domains, identify and prioritize network vulnerabilities, and facilitate secure threat intelligence sharing between the public and private sectors. By offering these technologies at a free or reduced cost, governments can ensure that even the smallest SMEs are equipped to defend against ransomware attacks.

Providing educational tools to SMEs can be equally effective for countries with limited funding. Resources like the United Kingdom's National Cyber Security Centre's (NCSC) Cyber Action Plan offer personalized security recommendations and training programs to help SMEs understand and implement critical security measures.

Leveraging International Development Funding

Latin American governments can seek funding from organizations like the Inter-American Development Bank (IDB) to support these initiatives.[85] The IDB provides financial and technical support to national and sub-national governments, focusing on development financing for health, education, infrastructure, and other key areas. By leveraging IDB's resources, countries can fund XDR and educational programs for SMEs.

The IDB's commitment to dedicating at least 35 percent of its annual lending approval volume to small and vulnerable countries in the region makes it an ideal partner for this endeavor. By accessing IDB funding, Latin American countries can ensure that SMEs have the necessary tools and knowledge to protect themselves against ransomware attacks, thereby enhancing regional cybersecurity and economic stability. However, governments must keep in mind that the funding process for the IDB can be lengthy and thus pose a risk to the efficiency of creating new initiatives.

Through a combination of regional cooperation, national initiatives, and international funding, Latin American governments can significantly bolster the cybersecurity resilience of SMEs. This multifaceted approach will mitigate the

[85] https://www.iadb.org/en

risks of ransomware attacks and promote a trustworthy and secure supply chain, fostering greater economic collaboration within the region and with allied nations like the United States.

External Funding Initiatives

The following recommendations highlight strategic alliances that both LATAM governments and the U.S. government can leverage to promote cybersecurity resilience among SMEs in the LATAM region.

Negotiating with Cybersecurity Providers

To promote economic opportunities and attract foreign investment, LATAM countries must demonstrate that their critical infrastructure is resilient. Thus, LATAM countries should focus on developing the appropriate incentives to attract companies providing XDR tools, encouraging them to provide access to their tools within a specified scope. Due to the structure of the digital ecosystem, keeping CI in the LATAM region secure depends on strengthening the capacity of SME suppliers. Including small suppliers in the scope of cybersecurity tools is crucial due to their uniquely vulnerable position, often stemming from a lack of technical expertise and limited resources. By ensuring small suppliers have access to robust cybersecurity measures, LATAM and the U.S. can enhance the overall security of reorganized supply chains. Recognizing the interconnectedness of the supply chain, as the U.S. NSA did with its CCC program, is crucial for LATAM's ability to attract foreign investment in the future.

If LATAM countries formed a coalition, they could use their collective power to negotiate with companies that provide XDR tools and services. These negotiations may be more difficult with a more established company like CrowdStrike, which may be less willing to yield an affordable price for LATAM countries. On the other hand, newer XDR companies, such as Expel, may be more open to negotiations with LATAM countries as agreeing to provide XDR services to SMEs in LATAM countries for a reduced price would enable them to scale and gain clients that otherwise would not be able to use their services. LATAM countries would benefit from convincing venture capitalists behind Expel that investing more capital to achieve a design-win in these countries would also yield benefits for the company.

The CHIPS and Science ACT

The CHIPS and Science Act, which aims to strengthen semiconductor supply chains, can be leveraged to fund cybersecurity programs in the LATAM region. The integration of Latin American countries in these supply chains creates an avenue through which funding from the CHIPS Act can be allocated to promoting cybersecurity resilience in the region.

Under a model in which LATAM governments form a coalition to negotiate with a cybersecurity services provider like Expel, funds from the U.S. and E.U. CHIPS Act or future industrial policy investments by the U.S. and Europe to evolve the semiconductor supply chain can potentially be used to subsidize any funds LATAM governments pull together for these services. The fact that this money would go to an American company, like Expel, would function towards ensuring that this funding model aligns with the CHIPS Act goals to strengthen technological capacity domestically.