DIGI AMERICAS ALLIANCE MEMBERS

REMARKS: NATIONAL CYBER DIRECTOR COKER AT LATAM CISO

The White House - It is a privilege and a pleasure to be speaking in front of such a distinguished group of cyber leaders and trusted partners from Latin America and the Caribbean. Your work is essential to protecting the shared values that our citizens cherish. Because we are living in a time of unprecedented opportunity. A time where the choices we make will shape the digital ecosystem for decades to come. President Biden has called this “a decisive decade.” And, to no surprise, I agree with him. We have a rare chance to collectively architect the systems that we want. Systems ensuring our mutual economic opportunity and regional security.

RODRIGO CHAVES CALLS FOR A MORE CYBER-SECURE LATIN AMERICA - LATAM CISO SUMMIT

DPL - Rodrigo Chaves, President of Costa Rica, called on Latin American countries to jointly build a region with greater cybersecurity through collaboration between countries. During the Latam CISO Summit 2024, Rodrigo Chaves welcomed the holding of events on cybersecurity, as he said that it is necessary to debate and share experiences to face the new challenges of cybersecurity. “Share your experiences, discuss the latest trends and challenges, and propose strategic solutions that strengthen our security in cyberspace in Latin America,” said the President of Costa Rica in an opening message.

MEXICO'S LEGISLATURE LACKS POLITICAL INTEREST AND KNOWLEDGE IN CYBERSECURITY: ALEJANDRA LAGUNES - LATAM CISO SUMMIT

DPL - The Mexican Legislature lacks the interest and knowledge to be able to approve a cybersecurity law, said Alejandra Lagunes, a senator in the last legislature. During the Latam CISO Summit 2024, Lagunes accused that the majority of legislators do not have the knowledge to recognize the importance of cybersecurity in economic, political and social life. “There is no political interest and there is little knowledge within the Legislature about cybersecurity,” said Alejandra Lagunes.

COSTA RICA WANTS TO BE THE ESTONIA OF LATIN AMERICA IN CYBERSECURITY: PAULA BOGANTES

DPL - “The cyberattack of 2022 brought us to our knees,” said Paula Bogantes, Minister of Science, Innovation, Technology and Telecommunications of Costa Rica. That is why governments must understand the importance of cybersecurity, while “Costa Rica wants to be the Estonia of Latin America in cybersecurity.” In 2022, the Central American country suffered a devastating cyberattack perpetrated by the Russia-linked Conti ransomware group. The attack affected multiple government institutions, paralyzing key services such as tax collection and customs, causing a nationwide cybersecurity crisis.

CYBERCRIMINALS ATTACK IN THE CLOUD AND USE ARTIFICIAL INTELLIGENCE: CROWDSTRIKE - LATAM CISO SUMMIT

DPL - Cybercriminals are moving to the Cloud and using Artificial Intelligence to attack countries' critical systems, warned Shawn Henry, Chief Security Officer of CrowdStrike. During the CISO Latam Summit, the executive of the cybersecurity company pointed out that supply chains, emerging technologies, incidents such as power failures, faulty software updates (referring to the one Crowdstrike had weeks ago) and natural disasters such as earthquakes, require organizations and companies to be more resilient.

RISK INTELLIGENCE PREDICTS CYBER THREATS AND PROTECTS THE BUSINESS - LATAM CISO SUMMIT

DPL - Cyber intelligence and cyber risk measurement allow for better decisions to be made to prevent vulnerabilities and cyber attacks and not affect businesses, agreed cybersecurity risk management specialists participating in the Latam CISO Summit 2024. Douglas Rocha, CISO (Chief Information Security Officer) of Banco BS2, explained that it is strategic to “translate cybersecurity risks to the Board of Directors” of companies. The key to data intelligence “is to explain how cybersecurity affects business.”

UNITED STATES INVESTS 300 MILLION DOLLARS FOR 5G IN COSTA RICA - LATAM CISO SUMMIT

DPL - The Export-Import Bank of the United States is providing $300 million to support Costa Rica's 5G initiatives, White House National Cybersecurity Director Harry Coker Jr. said. Costa Rica is in the process of bidding for 5G frequencies. The government of President Rodrigo Chaves published a decree on security for future 5G deployments, but it restricts suppliers of Chinese origin.

TRANSPARENT CLOUDS? A NECESSITY TO IMPROVE CYBERSECURITY - LATAM CISO SUMMIT

DPL - When there are security breaches and cyberattacks, it is necessary for companies, governments and Cloud providers to collaborate transparently in order to protect themselves, experts on the subject agreed during the Latam Ciso Summit 2024. Jason Merrick, senior vice president of Product at Tenable, asserted that everyone must be able to be transparent and exemplified this with the alliances that his company has with other Cloud providers. “We have to be able to provide transparency. We have alliances with Amazon, Palo Alto, to be able to share information and every time there is an incident we can work on it with our clients. It is about an ecosystem, sharing privileged information so that everyone knows what happened,” commented the executive.

CYBERCRIMINALS ATTACK IN THE CLOUD AND USE ARTIFICIAL INTELLIGENCE: CROWDSTRIKE - LATAM CISO SUMMIT

DPL - Cybercriminals are moving to the Cloud and using Artificial Intelligence to attack countries' critical systems, warned Shawn Henry, Chief Security Officer of CrowdStrike. During the CISO Latam Summit, the executive of the cybersecurity company pointed out that supply chains, emerging technologies, incidents such as power failures, faulty software updates (referring to the one Crowdstrike had weeks ago) and natural disasters such as earthquakes, require organizations and companies to be more resilient.

CYBERSECURITY SPECIALISTS ARE LACKING - LATAM CISO SUMMIT

DPL - “Cybersecurity is a human problem, but there are not enough people to defend us from cyberattacks,” said Mauricio Nanne, Director of Information Security at SISAP. He mentioned that we have to learn to defend ourselves from new cyberattack techniques, such as the use of Artificial Intelligence. The reason is because humans are IT professionals, but not yet cybersecurity professionals. These specialists are not disciplined to protect security every day.

THE FUTURE OF CYBERSECURITY REQUIRES A SPECIALIZED WORKFORCE: DAVID HOFFMAN - LATAM CISO SUMMIT

DPL - The digital future requires a cybersecurity workforce, said David Hoffman, professor of public policy at Duke University. Data has become increasingly complex and valuable, and cybersecurity is increasingly important to governments and organizations, so more experts are needed. Hoffman called for overcoming the underrepresentation of women in the cybersecurity industry and proposed a research program in the region to develop specialized cybersecurity talent.

MITIC CEO ANNOUNCES ISRAEL'S COOPERATION IN CYBERSECURITY - PARAGUAY

La Nación - In response to the recent reopening of the Israeli embassy in Paraguay, the head of the Ministry of Information and Communication Technologies (Mitic), Gustavo Villate, stressed that bilateral strengthening and strategic areas for national development will begin to be seen. “We will continue to strengthen ties, in fact, we have been working with Israel on issues of space cybersecurity, where they have an important strength. For us, working with our strategic allies is more than fundamental,” said the Secretary of State.

HACKING OF SAT WEBSITE IN SINALOA: IS ORGANIZED CRIME BEHIND THE ATTACK? THIS IS WHAT EXPERTS SAY - MEXICO

El Financiero - Cyber attacks on the websites of the Tax Administration Service of the State of Sinaloa (SATES) and the College of Bachelors of the State of Sinaloa (Cobaes) in which a 'narco message' is displayed compromise the personal information of the citizens of the entity, which is very dangerous because until now it is unknown if the group of cybercriminals is linked to criminal organizations in Sinaloa.

OPERATION KAERB: A CYBERCRIME NETWORK LED BY AN ARGENTINEAN IS DISMANTLED

R2820 - The Ministry of National Security highlighted that it managed to dismantle an International Cybercriminal Network whose actions begin with the theft of cell phones and are linked to various cybercrimes (such as unauthorized access, data theft, extortion, fraud). The recent Operation presented by the Secretary of Security, Alejandra Monteoliva, together with the intervening security forces, revealed the existence of a sophisticated criminal network dedicated to configuring a multitude of technologically assisted crimes, preferably high-end cell phones, in order to then obtain through deception the access credentials not only to the victim's device, but also to all of their information and applications.

GOVERNMENT JOINS EUROPEAN UNION INITIATIVE ON CYBERSECURITY AND CYBERCRIME - GUATEMALA

Prensa Libre - In a joint statement issued on Tuesday, September 17, the European Union (EU) in Guatemala and the Presidential Commission on Open and Electronic Government announced Guatemala's accession to the Latin American and Caribbean Cyber Competence Center (LAC4). According to both entities, this decision was made to support and improve the work of the Executive Branch's cybersecurity departments in the country, such as the National Cyber Security Committee, the Ministry of the Interior and the Ministry of Defense, among others.

WHAT WE KNOW ABOUT THE HEZBOLLAH PAGERS THAT EXPLODED IN LEBANON

CBS - A Hungarian official told CBS News Thursday that a Bulgaria-based company had purchased pagers from Taiwan that were eventually sold to Hezbollah, before exploding in the hands, pockets and bags of thousands of the Iran-backed militant group's members earlier this week in Lebanon. Hungarian outlet Telex had reported Wednesday that a Sofia-based company called Norta Global Ltd. Was behind a deal to sell the pagers and that a Hungarian firm connected with the transaction had not manufactured or sold the pagers. A Hungarian official told CBS News those reports were accurate. The new information about the origin of the exploding pagers came a day after Taiwanese company Gold Apollo said it had authorized the use of its trademarked branding on the pagers that exploded Tuesday across Lebanon and Syria, but that the devices were actually manufactured and sold by Bac Consulting KFT — a company based in Budapest, Hungary.

STRENGTHENING CYBERSECURITY: LESSONS FROM GUYANA'S DEFENCE INITIATIVE

Barbados Today - Technology can't be overlooked, especially with its rapid advancement, transforming warfare through innovations like combat drones. These advancements introduce new challenges and opportunities in the field of defence." With these words, Guyana's President Mohamed Irfaan Ali breathed life into what is likely the region's first National Defence Institute (NDI). The NDI, launched in Guyana, holds a broad mandate encompassing national security, including military strategy and tactics, with a key objective set by President Ali: to analyse gang movements and other transnational security threats. By addressing these cross-border challenges, the NDI underscores the need for regional cooperation, particularly in cyber defence and intelligence sharing. As the Caribbean faces increasing susceptibility to cyberattacks, the NDI is well-positioned to become a regional leader in cybersecurity preparedness.

SPOTIFY JOINS META IN OPEN LETTER TO EU DECRYING 'INCONSISTENT REGULATORY DECISION MAKING'

Digital Music News - Meta, Spotify, and several other companies and researchers have signed the open letter claiming that Europe has become less competitive and risks falling behind in the age of AI. The signatories seek "harmonized, consistent, quick and clear decisions" from data privacy regulators to "enable European data to be used in AI training for the benefit of Europeans." The letter specifically takes issue with the General Data Protection Regulation (GDPR) which passed in 2018. Specifically, Meta has stopped plans to harvest data from European users to train AI models after privacy regulators put pressure on the company and have issued fines for failing to respect privacy laws.

IS PATIENCE WANING WITH EFFORTS TO MODERATE CONTENT ON SOCIAL MEDIA?

WEF - Shortly after Hamas launched its surprise attack on Israel last October, channels used by the terrorist group on Telegram lit up with images of the ensuing atrocities. The response? A restriction of those channels that reportedly didn't do much restricting. Nearly a year later, Telegram's steady cultivation of a reputation as a free-speech bastion, sometimes to an extreme degree, has hit a glitch with the arrest of its founder and CEO in Paris. Pavel Durov has been compelled to remain in France, where he's under investigation for alleged complicity in criminal activity on his popular platform. "I got interviewed by police for 4 days," he posted on his channel. "No innovator will ever build new tools if they know they can be personally held responsible for potential abuse of those tools."

SDIM24: HOW PREVENTION-FIRST STRATEGIES AND ZERO TRUST CAN ENHANCE CLOUD SECURITY

WEF - In today's cloud-driven world, cyber security is a fundamental strategic consideration. CNAPPs have consequently gained popularity as a means of securing critical cloud environments. These security solutions are designed to protect cloud-native applications throughout their lifecycle, from development to deployment. Although CNAPPs help identify and manage risks, they primarily focus on alerting users and suggesting remediation rather than preventing attacks. As organizations rapidly adopt cloud technologies, the evolving threat landscape exposes the limitations of CNAPPs, making their security promises incomplete.