The Threat of Ransomware to Critical Infrastructure

Heriberto Acosta-Maestre, PhD

Oct 30, 2025

About Me

Bachelor's Degree: Computer Engineering at Polytechnic University of Puerto Rico

Master's Degree: Knowledge Discovery and Data Mining at Polytechnic University of Puerto Rico

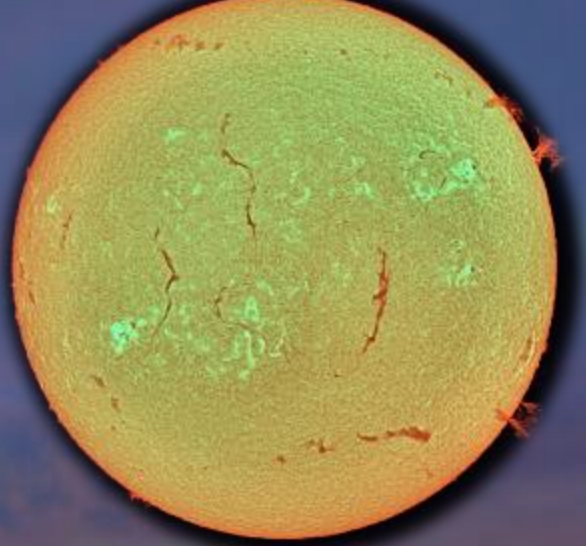
Ph.D.: Information Systems Security at Nova Southeastern University in Ft Lauderdale, Florida

Professional Experience: Worked as Technical Program Manager with the Puerto Rico National Guard (PRNG) for 15 years

Currently: Cyber Fellow at the WJPC (via Akima LLC)

Hobbies: Astrophotography, General Photography

Contact: Heriberto.Acosta@outlook.com



Disclaimer

The ideas contained in this presentation are the responsibility of its author and do not necessarily reflect the views or policies of WJPC, NDU, DoD, Akima LLC, or the U.S. government.

Agenda

Introduction:
Context about ransomware and critical infrastructure

Critical Infrastructure:
Definition (U.S. framework) and why it is vital

Ransomware and Essential Services:
Potential impact and global examples

Current Trends:
Types of ransomware attacks on critical infrastructure

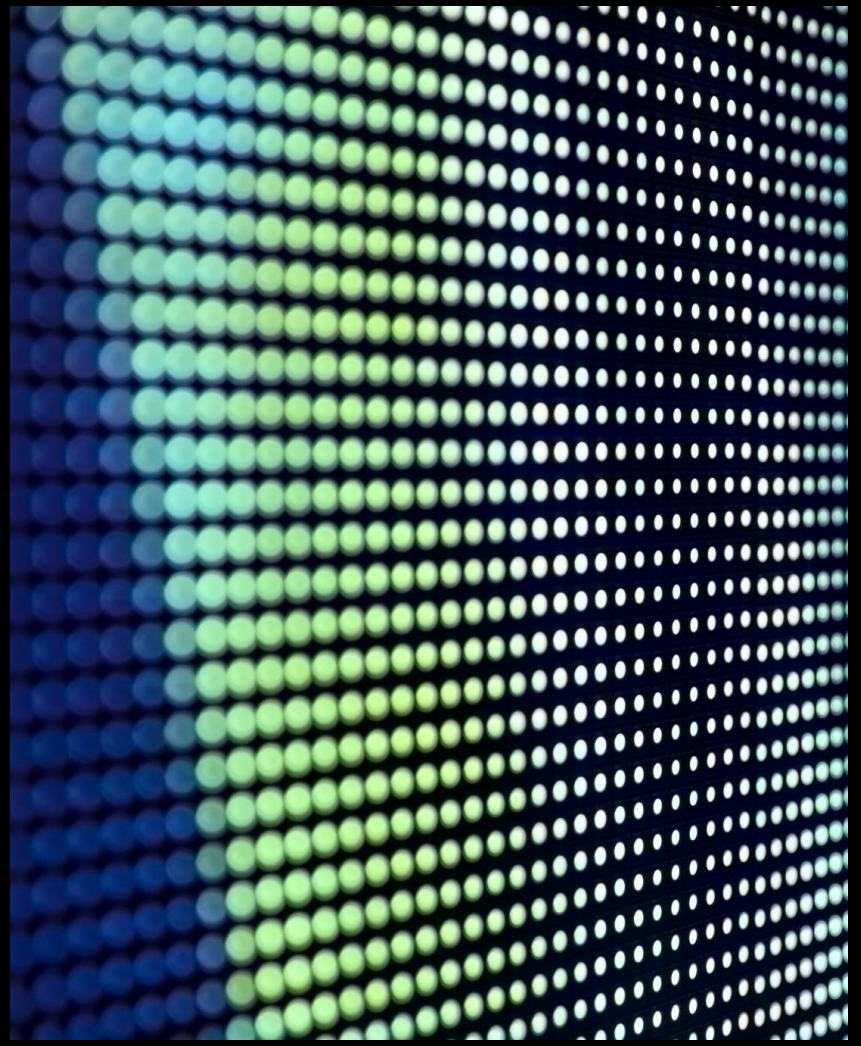
Panorama in Latin America:
Growing focus of cybercriminals in the region

Ransomware Groups:
Conti, LockBit, BlackCat, REvil, Clop, etc.

Recent Incidents and Implications:
Strategic, operational, and public policy implications

Recommendations:
Measures for governments and the private sector

Key Conclusions



What is critical infrastructure?

- **Critical infrastructure according to the U.S. framework**
- **16 sectors**
- These are systems and assets, physical or virtual, so vital to a country that their incapacity or destruction would have a debilitating impact on national security, economic stability, public health, or public safety.
- Fundamental services whose failure can put the functioning of the nation at risk in key areas.
- They are interdependent: an attack on one can trigger a domino effect in others.
- Their protection is a priority for national security.

Examples of critical sectors:

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Health and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

Importance of Protecting Critical Infrastructure

- **Social**
  - Essential services sustain daily life.
  - Prolonged disruption can cause chaos: massive blackouts, lack of water or fuel, collapse of communications.
- **Security**
  - Direct risk to human lives (example: inoperative hospitals).
  - Compromise of national defense and public safety.
  - Loss of trust in institutions.
- **Economic**
  - Costs of technical recovery plus losses due to interruption of operations.
  - Example: ransomware attack on Ireland's health system (2021) → suspension of medical services, direct costs > €80 million (estimated at ~€100 million).
- **Interdependence**
  - Critical infrastructures are interconnected.
  - An attack in one sector can trigger cascading failures in others.
  - This makes them high-value targets for cybercriminals and hostile state actors.

Ransomware in Critical Infrastructure

- Ransomware has become one of the greatest cyber threats for governments and businesses.
- Criminal groups encrypt critical data, demand multimillion-dollar ransoms, and apply double extortion by stealing confidential information.
- Critical infrastructure includes essential services such as energy, water, health, transportation, finance, and telecommunications, whose operation is vital for society.
- A successful ransomware attack can paralyze essential operations, compromise national security, and affect citizens' daily lives.
- In Latin America, cyberattacks; especially ransomware; have shown drastic growth in recent years.
- According to the Aon Global Cyber Risk Report 2025, ransomware claims in the region grew by 24% in one year.
- The report "The State of OT Cyber Security in LATAM 2024" warns that economic damages from cyberattacks exceed 1% of GDP in some countries and can reach up to 6% when critical infrastructure is affected.
- This growth is explained by rapid digitalization not accompanied by proportional advances in cybersecurity, leaving regional critical infrastructure highly vulnerable to malicious actors.

Global Examples – Ransomware Paralyzing Essential Services

- **Colonial Pipeline – USA (2021)**
- The DarkSide group launched a ransomware attack that forced the shutdown of the largest fuel pipeline on the East Coast, responsible for ~45% of the region's gasoline and diesel supply.
- 8,850 km of pipelines were disrupted, causing fuel shortages and panic buying in 17 states.
- The government declared a state of emergency.
- It was one of the most disruptive cyberattacks in the history of U.S. energy infrastructure, highlighting the vulnerability of interconnected industrial systems.
- **National Health Service – Ireland (HSE, 2021)**
- The Conti ransomware crippled the national health network.
- Hospitals had to return to the use of paper and pencil; Hundreds of surgeries and appointments were canceled.
- The full recovery took months and direct costs exceeded **€80 million**, with estimates close to €100 million.
- This case showed that hospital systems are priority targets for ransomware and that attacks have a direct impact on the lives of citizens.
- **Global lesson**
- Even developed countries have suffered severe consequences from ransomware in critical sectors.
- The response required extraordinary government action, including emergency declarations and federal intervention.
- Latin America must learn from these cases to strengthen preparedness and resilience in the face of similar threats.

Ransomware vs. Critical Infrastructure (Global Trend)

- **Increased attacks**
  - In 2023, 42% of ransomware incidents reported to the FBI affected critical infrastructure organizations.
  - This represents a significant increase compared to the 33% recorded in 2022.
- **Diversity of affected sectors**
  - Of the 16 critical sectors defined in the U.S., at least 14 reported ransomware victims in 2023.
  - The health and manufacturing sectors were among the hardest hit, but no sector is completely safe.
  - Attackers choose critical organizations with vulnerabilities, either to maximize the impact or increase the likelihood of payment.
- **Growth in losses**
  - Reported economic losses from ransomware in the U.S. grew 74% between 2022 and 2023, reaching approximately $60 million in 2023.
  - The real cost is higher, as it includes rescues, operational interruptions, system recovery and collateral damage.
- **Underreporting of incidents**
  - Only about 20% of victims officially report to the authorities.
  - This means that the actual incidence is much higher and that ransomware remains a latent threat to critical infrastructure.

Types of ransomware attacks against critical infrastructure

- **Double extortion (encryption + data theft)**
  - The most common strategy among large ransomware groups.
  - Attackers encrypt systems and steal sensitive information (power grid plans, medical records, etc.).
  - Even with backups, the threat of critical data release increases the pressure and amplifies the impact.
- **Operational disruption of control systems**
  - Ransomware can affect IT systems that are essential for physical operation (OT).
  - Although most incidents do not directly attack ICS/SCADA, companies preemptively stop services to prevent spread (example: Colonial Pipeline).
  - The risk of impact on industrial controllers is real and can force disruptions to critical services.
- **Attacks on third parties and suppliers (supply chain effect)**
  - Cybercriminals target IT, cloud, or telecom service providers that manage multiple critical customers.
- A single attack can impact dozens of organizations.
  - Example: IFX Networks (2023) affected 762 entities in Colombia, Chile, and Panama, including ministries, banks, and companies.
- **Destructive Ransomware (Wipers in Disguise)**
  - Malware designed to sabotage under the guise of ransomware.
  - Case in point: NotPetya (2017) in Ukraine, which paralyzed energy grids and other infrastructure with no intention of bailing out.
  - Although less frequent, it shows that ransomware can also be a weapon in hybrid warfare contexts.

“Ransomware-as-a-Service” (RaaS)

What is RaaS?

- Scheme in which ransomware developers rent their tools to "affiliates" (other cyber criminals).
- Affiliates launch the attacks and share the ransom payments with the developers.
- This model has democratized the threat: even attackers with low technical expertise can execute sophisticated campaigns.

Aftermath

- Huge increase in the number of groups and attacks.
- Example: **REvil** once had ~60 affiliates distributing its ransomware, making it one of the most active in the world.
- Other groups such as **Conti, LockBit, and Hive** have also operated under this model, allowing simultaneous attacks in different regions under the same "brand."

Professionalized criminal infrastructure

- RaaS operators offer affiliates:
  - Ready-to-use kits.
  - Command and control servers.
  - Operation manuals and technical support.
- Profit sharing: Affiliates usually keep **50–80% of the ransom,** the rest goes to the developers.
- Result: ransomware has become a **lucrative and scalable criminal industry.**

Implications for critical infrastructure

- The RaaS model multiplies the number of attackers capable of compromising essential services.
- Not only do a few elite groups pose a risk, but a **diverse and ever-changing criminal ecosystem.**
- Defenses must be reinforced in a broad and sustained manner to face this environment.

Common attack vectors and tactics

- **Initial access: phishing and stolen credentials**
  - Phishing emails with malicious files or links continue to be the most common way of entry.
  - The abuse of insecure remote access (e.g. unprotected RDP) has been massively exploited.
  - In 2020, more than **80% of successful attacks** involved compromised RDP credentials or brute force.
  - Teleworking during the pandemic expanded this attack surface, highlighting the need to secure remote connections.
- **Exploiting vulnerabilities in exposed systems**
  - Ransomware groups exploit unpatched software flaws in servers, VPNs, and critical internet-connected applications.
  - They have also used **zero-day** exploits in widely deployed products.
  - Agile patch management is vital: the speed of applying fixes can make the difference between being protected or being a victim.
- **Lateral mobility and quiet preparation**
  - Once inside, attackers move around the network to escalate privileges and reach critical systems.
  - They use legitimate tools (management scripts, common remote access Trojans) to evade detection.
  - They can stay inside the network for days or weeks, stealing credentials and disabling backups before detonating encryption.
- **Multiple extortion**
  - In addition to encrypting and exfiltrating data (double extortion), some groups apply a **third layer of pressure**: DDoS attacks against the victim's public sites.
  - Example: BlackCat/ALPHV launched denial-of-service attacks to pressure those who were late in paying.
  - This combination of **encryption + leakage + DDoS** seeks to corner critical organizations from all fronts.

Panorama in Latin America – What's Happening?

- **Accelerated increase in incidents**
  - LAC is today the region with the highest growth in cyber incidents worldwide.
  - Since 2013, it has registered an average annual growth of **~25% in reported incidents**, a trend that continues in the post-pandemic era.
  - In 2024 it was singled out as the fastest growing region in globally reported incidents.
  - Ransomware attacks **account for a significant portion** of this trend.
- **Higher exposure, lower protection**
  - Mass digitalization (digital government, IoT, online services) has not been accompanied by equivalent investments in cybersecurity.
  - LAC is listed as the **least protected region**, with an average score of **10.2/20** in cybersecurity compromises.
  - This gap leaves the region with **vulnerable targets and insufficient defenses.**
- **Critical infrastructure under attack**
  - In the last 3–5 years, several countries have suffered disruptive incidents against essential services: intentional blackouts, massive leakage of citizen data, attacks on banking systems, and ransomware on government agencies.
  - The region went from being a "secondary" target to a **key battleground in global cybersecurity.**
  - Emblematic case: **Costa Rica (2022)** declared **a national emergency** after a wave of ransomware against state institutions, becoming the **first country in the world** to do so due to a cyberattack.

Why is Latin America an attractive target?

- **Policy gaps and preparedness**
  - Only **7 out of 32 countries** have national plans to protect critical infrastructure from cyberattacks.
  - Only **20 countries have operational CSIRTs.**
  - The lack of coordinated protection frameworks and protocols makes the region fertile ground for attackers.
- **Limited resources and competing priorities**
  - Budgets focus on health, education, and public safety, leaving cybersecurity in the background.
  - Many organizations operate with nascent security programs and insufficient basic technical defenses (segmentation, 24/7 monitoring, rapid patching).
  - This opens up opportunities for cybercriminals to exploit known vulnerabilities.
- **Perception of low risk of retaliation**
  - Most ransomware groups operate from Eurasia, where attacking the US or Western Europe carries greater international pressure.
  - Latin America is seen as a target with less **probability of immediate punitive response.**
  - Limited legal and operational capacity in cybercrime reduces deterrence.
- **Accelerated digitalization without resilience**
  - After the pandemic, the region massively adopted teleworking, online procedures and electronic payments.
  - Cybersecurity did not grow at the same rate as connectivity (IoT, SCADA connected).
  - This creates a **"perfect storm"**: many exposed systems without patching or constant monitoring.
- **Recent successes that incentivize attacks**
  - Cases such as the **Conti and Hive attacks in Costa Rica (2022)** demonstrated the effectiveness of extorting Latin American governments.
  - Leaks of valuable data (e.g., citizen records) have generated profits on black markets.
  - The region's reputation as **a profitable and vulnerable target** circulates on criminal forums, attracting groups such as **LockBit and BlackCat.**

Top Ransomware Groups (I)

LockBit

- Currently the most prolific group worldwide, with a strong presence in the region.
- It operates under the **RaaS model** and leads with **59 attacks in LATAM** in the last period analyzed (2024).
- Victims: from government agencies to industrial companies.
- Distinctive features:
  - Effective software (LockBit 3.0 variant).
  - Aggressive **double extortion** strategies.
  - Continuous expansion through affiliates.
- Considered the **biggest ransomware threat** currently.

ALPHV / BlackCat

- Active since the end of 2021, successor to BlackMatter/DarkSide.
- Pioneer in using **Rust language**, making it difficult to detect.
- He innovated with the free publication of stolen data to pressure.
- In Latin America it has had a strong impact, especially in **Mexico** (>1000 organizations affected).
- It usually employs **triple extortion** (encryption, filtering, and DDoS).
- Although it suffered disruptions in 2023, it is still active globally with very technical affiliates.

Clop

- Known for massive **zero-day attacks** on third-party software.
- Example: operation of **MOVEit servers** in 2023.
- It operates as **a RaaS**, with a focus on extortion data breaches.
- Strategy: Engage suppliers to impact multiple victims at once.
- Although less publicized than LockBit, it has been behind **high-profile breaches** and continues to be active.

Jellyfish

- Emerging group observed in 2023 with a focus on the region.
- Emblematic case: attack on the **National Securities Commission of Argentina** (June 2023).
- Characteristics:
  - Ransom note "!! READ_ME_MEDUSA!!!"
  - Files encrypted with **. MEDUSA.**
- He also claimed attacks against **Garbarino (Argentina)** and mentioned victims in **Bolivia, Brazil, Chile, Colombia and the Dominican Republic.**
- Although smaller, its **regional focus and diversity of sectors** make it a group to watch closely.

Top Ransomware Groups (II)

Conti

- One of the most feared bands until its dissolution in 2022.
- Responsible for high-profile attacks, including the massive coup against the **government of Costa Rica.**
- Famous for multimillion-dollar lawsuits and data leaks, he even threatened to overthrow the Costa Rican government.
- After the leak of its internal chats (*Conti Leaks*) and international pressure, it announced its closure.
- Many members migrated to other groups such as **BlackCat** and **Hive.**
- Legacy: It left chaos in the region and forced improvements in government cyber resilience.

Hive

- Active between 2021 and 2022, with a focus on the **health sector and public agencies.**
- Emblematic attack: **CCSS (Costa Rica, 2022),** which affected hospitals and medical records.
- He applied **double extortion** and used very efficient malware.
- The FBI infiltrated its infrastructure for months and in January 2023 announced its dismantling, releasing decryption keys to victims around the world.
- Its affiliates then migrated to other RaaS programs.

.

REvil (Sodinokibi)

- RaaS Group very active between 2020 and 2021, with dozens of affiliates.
- Emblematic cases:
  - **JBS Foods** (Brazil, paid from ~11 MUSD).
  - Chain attack via **Kaseya.**
- It attacked companies in Brazil, Mexico and other countries.
- Pressure from the US led Russian authorities to announce its dismantling in 2022.
- Although its activity fell, it set a trend in extortion and laid the foundations for new groups

Top Ransomware Groups (III)

- **DarkSide / BlackMatter**
  - DarkSide was responsible for the attack on the **Colonial Pipeline (USA, 2021).**
  - Following worldwide attention, he announced his retirement, but briefly reappeared as **BlackMatter.**
  - Main objectives: energy and industry.
  - Attacks on a hydroelectric plant in Chile (2021) and agro-industrial cooperatives in the US are attributed to him.
  - It ceased operations at the end of 2021 citing police pressure.
  - Its modus operandi (focused on physical infrastructures) inspired later groups.
- **Final note**
  - The 'brand' of ransomware groups is volatile: they disband, rename, or resurface.
  - Example: after the disappearance of **Conti** and **Hive**, its members were integrated into **BlackCat, Royal** and other variants.
  - These groups left a significant mark on global **and Latin American critical infrastructure**.

Case 1 – Costa Rica 2022 (Hack Accounts)

Context

- In April 2022, Costa Rica suffered a devastating attack by the **Conti** group, targeting multiple state agencies simultaneously.

Affected organizations

- At least **27 government entities** were infiltrated, including:
  - Ministry of Finance (finance and taxes).
  - Ministry of Labor.
  - Social security.
- Tax, customs, human resources and public procedures systems were disabled.

Demands and actions

- Conti demanded **US$10 million** in ransom.
- The government refused to pay.
- In retaliation, the attackers gradually leaked **~97% of 672 GB** of stolen data, exposing sensitive information of citizens and officials.

Impact and duration

- State operations affected for almost **two months.**
- **Tax collection and international trade paralyzed,** with serious economic effects.
- A cost equivalent to **2.4% of the national GDP** is estimated.

Extraordinary response

- The president declared **a state of national emergency,** the first time in the world due to a cyberattack.
- Emergency funds were activated and assistance was received **from the U.S.,** including reward for Conti leaders.

Lessons

- A criminal group managed **to bring a state to its knees.**
- Urgency to strengthen the security of critical government systems.
- The need for international cooperation to confront these threats.
- Escalation in criminal rhetoric: Conti went so far as to threaten to **"overthrow the government."**
- With external support, Costa Rica gradually restored systems, leaving this case as a **global milestone of ransomware against a State.**

Caso 2 – Costa Rica 2022 (Hive Hack)

Context

- Just weeks after Conti's attack, in May 2022, Costa Rica was hit by Hive ransomware, targeting the **Costa Rican Social Security Fund (CCSS).**
- The CCSS is the pillar of the country's public health: hospitals, clinics and medical records.

Scope of the attack

- Critical hospital IT services were **encrypted.**
- Hospitals lost access to:
  - Patient databases.
  - Laboratory and pharmacy systems.
- Staff had to resort to **manual processes.**

Impact on the population

- Cancellation and delay of **appointments, surgeries and treatments.**
- Physicians without access to medical records.
- Delays in test results (including COVID-19).
- Suspension of online appointment issuance and payment of pensions.
- Thousands of citizens affected in their health and daily lives.

Answer

- The government refused to pay ransom.
- With international support (including the **FBI)** systems were restored from backups.
- The national emergency already declared by Conti was extended to cover the **health sector.**

Outcome and police action

- Hive leaked some data to press.
- In January 2023, the **U.S. Department of Justice.** announced the **dismantling of Hive**, after infiltrating its operation and releasing decryption keys to victims around the world.
- The attack on Costa Rica was one of the triggers for this international operation.

Lessons

- The double crisis of Conti and Hive showed the **vulnerability of multiple critical sectors in the same country.**
- He underscored the **interconnectedness of threats**: Hive's collapse was driven by its global impact.
- For Costa Rica, it resulted in urgent improvements:
  - Creation of a **national CSIRT.**
  - Investment in **offline backups.**
  - **Segmentation of critical hospital networks .**

Case 3 – Colombia 2023

Context

- In September 2023, a ransomware attack against **IFX Networks,** a provider of cloud services and datacenters in 17 countries, caused a cascading effect in the region.
- The ransomware used was identified as **RansomEXX** (or similar variant).

The incident

- The attackers encrypted the **virtualization servers,** taking the Infrastructure-as-a-Service **(IaaS) platform offline.**
- The drop affected both public and private customers.

Affected entities

- **20 Colombian public entities paralyzed** and another 78 with interruptions.
- More than **762 private companies** affected in Colombia, Chile, Panama, Argentina and other countries.
- Concrete impact:
  - **Colombian Foreign Ministry** → temporary suspension of visas and passports.
  - **Judicial branch** → the procedures portal crashed.
  - Universities, banks and digital providers affected.

Crisis response

- The Colombian government declared the incident a **national digital security issue.**
- Contingency plans and migration of critical services to alternate infrastructure were activated.
- Response teams worked 24/7 alongside IFX; Recovery took more than a week.

Regional dimension

- The attack showed the **risk of concentration** in a single service provider.
- The fall of IFX simultaneously impacted **several countries in the region,** a rare occurrence.
- Governments of Chile and Panama issued alerts and offered assistance to their affected institutions.

Lessons

- An attack on a **common provider** can morph into a regional critical infrastructure event.
- Organizations should:
  - Assess **third-party risks.**
  - Have **contingency plans** in place in case of supplier failure.
  - Review the **resiliency of critical cloud services** and geo-segmentation of backups.

Case 4 – Chile 2023

Context

- On October 23, 2023, the Chilean company **GTD**, a telecommunications, cloud, and data center provider, suffered a ransomware attack.
- The malware identified was **Rorschach (aka BabLock),** a rare variant.
- The attackers encrypted the **Infrastructure as a Service (IaaS) platform**, forcing the suspension of cloud services.
- **Disrupted Services**
- More than **3000 customers affected**, including private companies and public entities in Chile and Peru.
- Impact on:
  - Data center.
  - IP telephony.
  - Corporate VPN.
  - Internet connectivity.
- Days after the attack, more than 300 customers were still experiencing significant problems.

Communication and regulations

- GTD handled the incident with **transparency and collaboration** with authorities.
- The case occurred shortly after the entry into force of the Chilean regulations on mandatory **notification of incidents** in state entities.
- GTD coordinated reports with its government clients, exemplifying **good response practices.**

Recovery

- Proactive suspension of services slowed the spread of ransomware.
- Restore backups and harden systems before reactivating the platform.
- In about **a week** , most services were restored, although there was **loss of unbacked data** in some customers.

Lessons

- The case reinforces the importance of **security in critical service providers.**
- Even advanced technology companies are vulnerable.
- The fall of a vendor affects an entire **ecosystem of dependent organizations**.
- GTD's **rapid response and clear communication** helped contain damage, showing the value of robust response plans.

Case 5 – Argentina 2023

Context

- In June 2023, the **National Securities Commission (CNV),** the regulator of Argentine financial markets, suffered a ransomware attack.
- The **Medusa group** claimed responsibility for the attack, which was officially confirmed on June 11.

The incident

- Network entry, server encryption, and theft of confidential information.
- The CNV isolated its systems and **suspended online platforms** to contain the spread.
- Digital capital market procedures (authorizations, reports, stock market consultations) were out of service for several days.

Impact

- Concern in the financial sector about the possible leakage of data from **listed companies and investors.**
- Risk of loss of confidence and possible effects on market stability.

Data exfiltration

- Medusa stole a significant volume of documents.
- He posted samples on his dark web site, including internal reports and personal data.
- He also mentioned other companies from Argentina and neighboring countries, evidencing a **regional campaign.**

Answer

- The CNV worked with the cybercrime unit to investigate the attack.
- Backup systems and recovery procedures were strengthened.
- No ransom payment was recorded; Some of the stolen information was published by the attackers.

Lessons

- Regulatory **bodies** are also strategic targets.
- An attack on a financial regulator can have **systemic effects**: loss of trust and even market manipulation.
- It is necessary that **good banking cybersecurity practices** also be extended to supervisory entities.
- It confirms Medusa's active presence in the region, targeting critical targets beyond the central administration.

Case 6 – Brazil 2020

Context

- On November 3, 2020, the **Superior Tribunal de Justiça (STJ),** Brazil's second-highest court, suffered a ransomware attack.
- The attack occurred during a virtual trial session.

The attack

- RansomUX-linked group compromised the court's network.
- More than **1,200 servers** (mainly virtual machines) were encrypted.
- The attackers **destroyed backups** to prevent recovery.

Suspension of activities

- All court sessions (virtual and face-to-face) were suspended for a week.
- **Procedural deadlines** and electronic access to files were paralyzed.
- The president of the STJ publicly reported the attack and involved the **Federal Police** from the beginning.

Cascade effect

- Other interconnected federal agencies were preemptively affected.
- Several ministries disconnected their links with the judicial network for security.

Research and response

- The attackers exploited a **domain administrator account** to spread.
- There was persistence prior to the detonation, which facilitated mass encryption.
- RansomEXX ransom note was found, but the court **did not pay ransom.**
- With the support of the **Federal Supreme Court,** systems were restored with **external backups** and manual reconstruction.

Lessons

- It was the **most serious cyberattack against a Brazilian public institution** to date.
- It highlights the importance of:
  - Target critical networks.
  - Keep **offline backups up to date.**
- It showed that **justice is also a target of ransomware,** directly affecting citizens' access to justice.
- Following the attack, Brazil created specific protocols to **protect digital judicial infrastructure.**

Latin America Incident Overview – Impact and Trends

Governments in the crosshairs

- Ministries, judicial courts and public entities are priority targets.
- A paralyzed government generates enormous pressure to negotiate and great media impact.
- Emblematic case: **Costa Rica**, the first country to declare **a national emergency** due to a cyberattack.

Essential services affected

- Health (Costa Rica), telecommunications (Chile, Colombia), finance (Argentina), justice (Brazil).
- Tangible impacts: lines at gas stations, patients without care, detained courts, risk of economic instability.
- It confirms that **all strategic sectors** are vulnerable.

High economic costs

- Costa Rica: losses estimated at **2.4% of GDP**.
- IFX Networks: companies and ministries with disrupted operations.
- Incidents show that **not investing in cybersecurity is more costly** in the long run.

Cooperation and intelligence sharing

- Examples: support from the **FBI in Costa Rica**, international operation against **Hive**, regional coordination after the IFX case.
- No country can face these threats alone.
- Cooperation with governments and the private sector is essential to mitigate large-scale attacks.

Need to improve preparedness

- Common gaps: unpatched systems, compromised credentials, lack of network segmentation.

Lessons:

  - Countries with **external backing** and **defined crisis protocols** recovered faster.
  - Improvisation delayed recovery in other cases.
- Cross-cutting message: **investing in preparedness and resilience is crucial**.

Strategic Implications - National and Defense Level

Threat to sovereignty and national security

- Mass attacks can weaken the state's ability to ensure basic services.
- Compromised sectors such as energy, telecommunications and finance leave the country vulnerable to external coercion.
- A cyberattack can degrade **military readiness** without firing a single bullet.
- Security doctrines must consider ransomware on the same level as physical threats.

Risk of social and political instability

- Prolonged disruptions to water, electricity, health or transportation can lead to **protests, panic and loss of trust in the government**.
- In fragile democracies, it can lead to political crises.
- Although attackers seek profit, their actions can destabilize governments.
- **Governance and crisis communication plans** are required in the face of major attacks.

Convergence with hostile state actors

- Adversary states could **sponsor or cloak behind ransomware groups** for geopolitical purposes.
- World Bank: **59% of incidents in developing countries would be politically motivated**.
- It blurs the line between cybercrime and cyberwar.
- Possible hybrid **war scenario**, using ransomware as a weapon to cripple infrastructure.

Need for national cyber defence policies

- Comprehensive national strategies with a focus on critical infrastructure.
- Define roles and responsibilities: Who leads in a serious national cyberattack?
- It requires **civilian-military-private coordination.**
- Creation of **specialised cyber defence units** and carrying out **national simulation exercises.**

Diplomacy and international cooperation

- Participation in global anti-ransomware initiatives (e.g. **U.S.-led initiative**).
- Joint intelligence sharing and training.
- Make critical **infrastructure cybersecurity** a recurring topic in multilateral forums (OAS, UN).
- Only an **international common front** can deter attackers and put pressure on states that tolerate them.

Operational implications - Organizations and industries

Prolonged business disruption

- Ransomware can halt operations **for days or weeks**, far beyond what was foreseen in traditional continuity plans.
- Cases: pipeline closed for 5 days, Brazilian court for 1 week, Costa Rican government for 2 months.
- It requires **rethinking BCPs** with extreme scenarios and manual contingency plans.

Data loss and trust

- Even if systems are restored, the **confidentiality and integrity** of the information can be compromised.
- Sensitive data exposed (energy, health, finance) leads to lawsuits and loss of public trust.
- A critical supplier's reputation can be severely eroded.

Unexpected operating costs

- Recovery involves overtime expenses, consultants, equipment, and audits.
- It forces **you to update obsolete infrastructure** in an accelerated manner.
- It can generate financial losses and a drop in shareholder value (example: Telecom Argentina, 2020).

Need for robust response protocols

- Many entities lacked specific anti-ransomware plans.
- Keys: isolate networks quickly, communicate effectively, coordinate with authorities, decide on payment/non-payment.
- Companies with **24/7 SOC** better contain attacks, reducing damage and attacker dwell time.

Supply chain disruption and contractual obligations

- The fall of a critical supplier generates **cascading effects** on customers and partners.
- Breaches of contracts, penalties and loss of commercial confidence.
- More and more contracts include **cybersecurity SLAs** and immediate notice clauses.
- Resilience is also a **criterion for selecting suppliers**.

Organizational Culture and Training

- Cybersecurity isn't just an IT issue – it needs to permeate the entire organization.
- Trained employees are the first line of defense against phishing and human error.
- Attack simulations and **red team/blue team** exercises strengthen preparation.

Implications for public policies and regulations

Updating legal frameworks

- Many countries still lack laws that require critical companies to implement cybersecurity measures or report incidents.
- It is urgent to develop specific regulations for the protection of critical infrastructure, with:
  - **Minimum safety standards.**
  - **Mandatory audits.**
  - **Fines for gross negligence.**
- Include legal mechanisms to facilitate **public-private cooperation** during incidents.

Centralization and national coordination

- Create or strengthen a **national cybersecurity authority** with a mandate on critical infrastructure.
- Define the priority sectors in each country (e.g. energy, finance, transport, health).
- Establish **specialized Response Teams** (sectoral or multi-sectoral).
- Today only **7 countries in the region** have dedicated plans for infra-critical.

Incentives and support for the private sector

- Most critical infrastructures are operated by **private companies.**
- Possible incentives:
  - Tax benefits for investments in security.
  - Joint training programs.
  - Threat intelligence sharing.
- Promote **public-private partnerships (PPPs)** in cybersecurity.
- Example: In the US, **sectoral ISACs** allow rapid alerts to be disseminated among critical companies.

Non-payment vs. save services policy

- Define in advance the national position on the **payment of ransoms**.
- Costa Rica, for example, maintained the policy of not paying despite the great impact.
- It is necessary to establish clear protocols for cases where **human lives are at immediate risk.**
- Evaluate options such as the **legal prohibition of payments**, already discussed in some countries.

International cooperation and joint frameworks

- Participate in global anti-ransomware initiatives and multilateral forums (OAS, UN).
- Promote **mutual legal assistance** (extraditions, judicial cooperation).
- Consider **public attribution** of attacks when there is foreign state support.
- Critical cyberattacks can escalate to the diplomatic level:
  - Example: after **Colonial Pipeline**, the US put pressure on Russia.
  - In LATAM, **Costa Rica sought international support** against Conti and Hive.

Recommendations for Governments and the Public Sector

National Cybersecurity Strategies

- Design plans with a focus on **critical infrastructures.**
- Include national inventory, risk analysis and sectoral protection plans.
- Create **multisectoral committees** that integrate civilian and military agencies and regulatory entities.

Institutional strengthening

- Establish or strengthen **national CSIRT/CERTs** with infracritical scope.
- Provide them with **expert personnel, sufficient budget and sectoral links** for rapid response.
- Invest in **training cybersecurity talent** (academic programs and certifications).

Regulatory and normative framework

- Oblige infra-critical operators to apply controls aligned with **international standards** (ISO 27001, NIST CSF).
- Require **continuity and incident response plans** specific to cyberattacks.
- Implement **mandatory reporting** of relevant incidents within a defined timeframe.
- Use the **OAS as a guide** to harmonize regional regulations.

Investments in resiliency and redundancy

- Financing the modernization of **obsolete systems** (ICS, hospitals, etc.).
- Ensure **offline backups** and alternative manual plans.
- Decentralize critical services (e.g. **alternate national data centers**).

High-level exercises and awareness

- Conduct **periodic national cyberattack drills** on critical infrastructure.
- Involve ministers, armed forces and CEOs of strategic sectors.
- Integrate cybersecurity into the **presidential and cabinet agenda.**
- Awareness from the top ensures political priority and resources.

Final note

- These measures seek **to raise the national defensive posture** and close the regional preparedness gap.
- They require **sustained political will** and **public-private collaboration.**

Recommendations for Private Operators of Critical Infrastructure

Good practice frameworks

- Adopt recognized standards (NIST CSF, IEC 62443 for industrial environments).
- Cover all functions: **identification, protection, detection, response, and recovery.**
- Measure and continuously improve the level of maturity in cybersecurity.

Segmentation and protection of industrial systems

- Separate **corporate IT** and **industrial OT networks** with secure gateways and monitoring.
- Apply **Zero Trust** principles: no connection is trusted by default.
- In plants, use **safe jump servers** and ensure manual operation capacity in case of a fall.

Robust backups and recovery plans

- Maintain frequent, encrypted backups stored **offline.**
- Periodically test restoration in simulated environments.
- Have a **Disaster Recovery Plan (DRP),** with alternate centers or recovery agreements.

Staff training and awareness

- Train at all levels in digital hygiene: **phishing, MFA, secure passwords.**
- Internal drills (simulated phishing, red team/blue team).
- Foster a **culture of early reporting** without blame.

Incident Response Capability

- Have an **internal CIRT** or an agreement with specialized providers.
- Clear procedures: isolation, preservation of evidence, communication with authorities.
- Define protocols for interacting with attackers under legal supervision.

Third-Party and Cyber Insurance Assessment

- Review the security of **critical suppliers** (audits, certifications).
- Consider **cyber insurance** as a risk transfer mechanism.
- The assurance process helps to detect gaps and raise internal controls.

Key message

- The private sector must operate under the logic of **"when it happens, not if it will happen".**
- Investment in prevention and resilience is minimal compared to the cost of catastrophic disruption.

Conclusion

Ransomware: A Strategic Threat

- It has established itself as one of the most serious threats to **critical infrastructure**, with effects comparable to natural disasters or terrorist acts.
- It can paralyze governments, slow down justice, cut off fuel, and compromise public health.

Latin America in the crosshairs

- It is the **region with the highest growth in cyberattacks** but with lags in protection.
- This has made it a priority target for criminal gangs.
- Recent incidents have raised awareness **of the problem**, creating an opportunity to turn alert into action.

Comprehensive and collaborative approach

- Isolated responses are not enough: **cooperation between governments, the private sector and international partners** is required.
- Early **coordination**, **intelligence sharing,** and **incident reporting** are key to crisis containment.

Readiness and resilience

- Organizations must assume that **they will eventually be attacked.**
- Those who invest in security and planning reduce the impact; those who improvise multiply it.

Protection of society and sovereignty

- Defending critical infrastructure is protecting **daily life, the economy and national sovereignty.**
- It is a technical challenge, but above all strategic **and managerial.**
- Military, government, and private leaders have a central role to play in driving improvements.

Final conclusion

- Cybersecurity **of critical infrastructures** must be treated as a **top national priority.**
- The next few years will be decisive in closing the gap in Latin America.
- With **political will, investment, and cooperation,** it is possible to build a safer and more resilient future against ransomware.

The end! Thank you for your time!