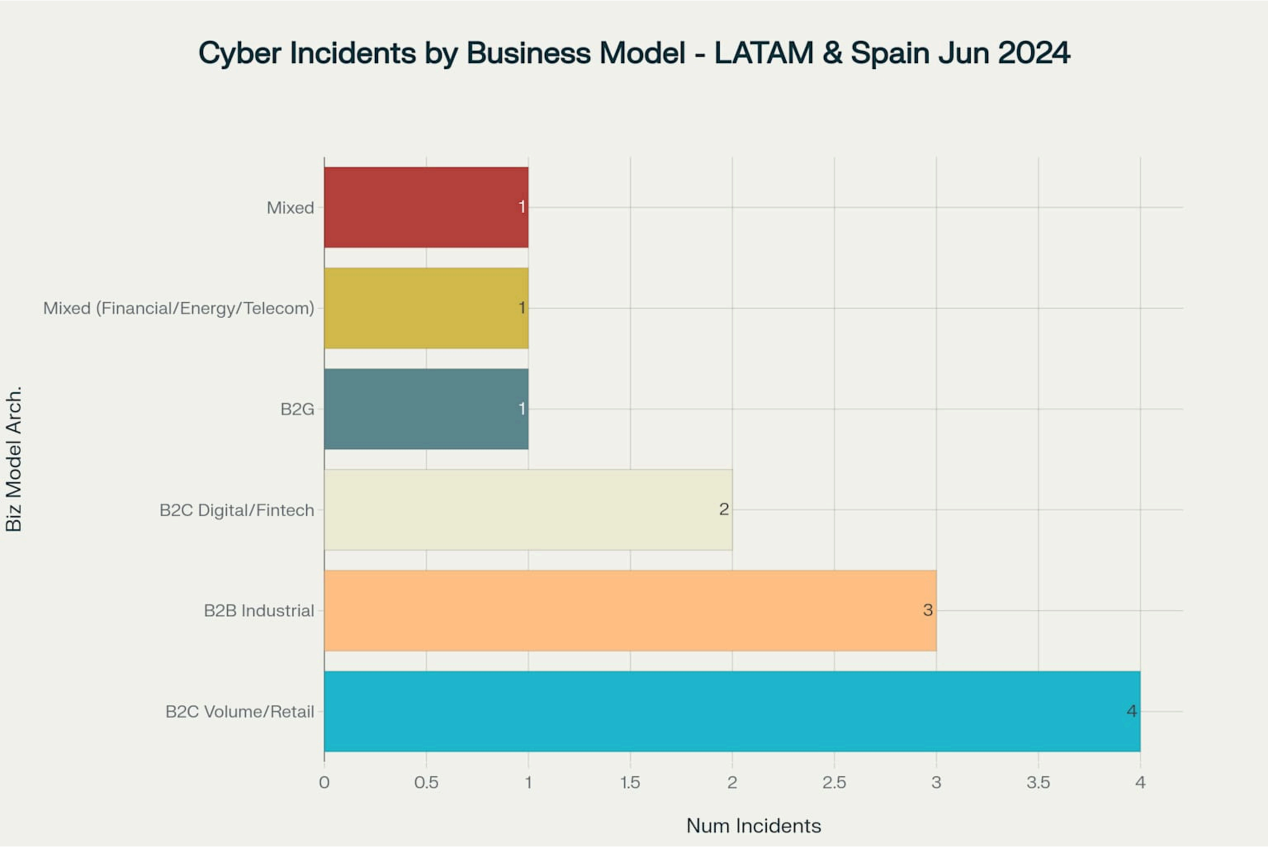
Cyber Incidents in LATAM and Spain: Business Model Vulnerability Analysis (June 2024)

Executive Summary

Analysis of confirmed cyber incidents in Latin America and Spain during June 2024 reveals a concerning pattern of successful attacks across all major business archetypes. **B2C Volume/Retail companies** emerged as the most frequent targets (4 incidents), followed by **B2B Industrial** organizations (3 incidents). The month saw several high-profile breaches affecting millions of customers, with attack success rates near 100% across all business models except government entities.



Distribution of confirmed cyber incidents across different business model archetypes in LATAM and Spain during June 2024, showing B2C Volume/Retail and B2B Industrial as the most targeted sectors.

Major Confirmed Incidents by Business Archetype

B2C Digital/Fintechs

Santander Bank (Spain) - May 14, 2024[1][2][3]

- **Attack Vector**: Third-party database breach via Snowflake compromise
- **Impact**: 30 million customer records plus employee data exposed across Chile, Spain, and Uruguay
- **Financial Impact**: Estimated millions in remediation costs
- **Threat Actor**: ShinyHunters group claimed responsibility
- **Data Exposed**: Bank account details, credit card numbers, HR information

C&M Software (Brazil) - July 1, 2024[4][5]

- **Attack Vector**: Fraudulent use of client credentials
- **Impact**: Six financial institutions affected with unauthorized access to reserve accounts
- **Financial Impact**: No client losses reported, but central bank intervention required
- **Operational Impact**: Brazil's central bank ordered shutdown of financial institution access

B2C Volume/Retail Companies

Telefónica (Spain) - June 3, 2024[6][7][8]

- **Attack Vector**: Data breach affecting Peruvian operations
- **Impact**: 120,000 users affected in Spain; 1 million customer records in Peru
- **Threat Actor**: "Dedale" hacking group claimed 22 million total customer records
- **Status**: Investigation ongoing despite sale of Peruvian operations in April 2024

Iberdrola (Spain) - May 30, 2024[9][10]

- **Attack Vector**: Third-party supplier security breach
- **Impact**: 850,000 customers (8% of user base) - 600,000 from Iberdrola Clientes, 250,000 from Curenergía
- **Data Exposed**: Names, surnames, ID numbers, contact details
- **Operational Impact**: Data being sold on Telegram forums and dark web platforms

LATAM Airline - June 2024[11]

- **Attack Vector**: Akira ransomware deployment via SSH protocol
- **Impact**: Critical data exfiltration before encryption
- **Threat Actor**: Storm-1567 (Punk Spider/GOLD SAHARA) ransomware group
- **Method**: Double-extortion tactics with Living off-the-Land techniques

B2B Industrial

Geopost Spain (DPD) - June 14, 2024[12]

- **Attack Vector**: Unauthorized database access by subsidiary in Spain
- **Impact**: Customer transport service data including names, addresses, emails, phone numbers
- **Response**: Immediate notification to Spanish cybersecurity authorities (INCIBE and AEPD)
- **Risk**: Potential for spam and phishing campaigns using stolen data

Santa Barbara Systems (Spain) - June 5, 2024[13][14]

- **Attack Vector**: Distributed Denial-of-Service (DDoS) attack
- **Threat Actor**: NoName pro-Russian hacktivist group
- **Target**: Spanish defense contractor refurbishing Leopard tanks for Ukraine
- **Impact**: Website offline, operations disrupted
- **Geopolitical Context**: Part of broader campaign against Spain's military support for Ukraine

B2G (Business-to-Government)

DGT - Directorate-General for Traffic (Spain) - May 31, 2024[15][16][17]

- **Attack Vector**: Suspected database unauthorized access
- **Impact**: Potentially 27-34.5 million driver records (entire Spanish driving database)
- **Data at Risk**: License plates, vehicle information, insurance details, personal identification
- **Status**: Under investigation by Guardia Civil; hackers offering database for sale on BreachForums
- **Timeline**: Suspicious activity detected May 13, data offered for sale May 13

Platform Companies

Spanish Ibex 35 Companies - June 2024[18][19]

- **Targets**: Multiple major Spanish corporations including Banco Santander, Telefónica, Iberdrola
- **Attack Vector**: Coordinated wave of cyberattacks
- **Context**: Part of broader trend with cyberattacks tripling compared to 2022
- **Sectors Affected**: Financial services, telecommunications, energy
- **Attribution**: Cyberattacks attributed to increased geopolitical tensions and digital transformation vulnerabilities

Attack Vector Analysis

Most Common Attack Methods

1. **Database/Data Breaches** (75% of incidents)
   - Direct database access through security vulnerabilities
   - Third-party supplier compromises affecting multiple downstream clients
   - Cloud service provider breaches (Snowflake incident affecting multiple organizations)
2. **Third-Party Supply Chain Attacks**
   - Geopost incident via Spanish subsidiary
   - Iberdrola breach through external supplier
   - Santander compromise via Snowflake cloud provider
3. **Ransomware Operations**
   - Akira ransomware targeting LATAM airline industry
   - Double-extortion tactics combining data theft with encryption
4. **State-Sponsored/Hacktivist Attacks**
   - NoName group targeting Spanish defense contractors
   - Attacks correlated with geopolitical tensions over Ukraine support

Financial and Operational Impact Assessment

High-Impact Incidents (>1M Records)

- **Santander Bank**: 30+ million records, estimated millions in remediation
- **DGT Spain**: 27-34.5 million potential records at risk
- **Telefónica Peru**: 1 million confirmed customer records

Medium-Impact Incidents (100K-1M Records)

- **Iberdrola**: 850,000 customer records
- **Telefónica Spain**: 120,000 user records

Operational Disruptions

- Central bank intervention (C&M Software Brazil)
- Website takedowns (Santa Barbara Systems)
- Customer warning campaigns (Iberdrola)
- Police investigations (DGT Spain)

Correlation Between Business Model and Attack Success

Key Vulnerability Patterns

B2C Digital/Fintechs show the highest individual impact scale, with Santander's 30 million affected records representing one of the largest financial sector breaches globally. These organizations face sophisticated threat actors targeting high-value financial data[1][3].

B2C Volume/Retail companies demonstrate consistent vulnerability across telecommunications and energy sectors, with attackers exploiting both direct system access and third-party suppliers. The frequency (4 incidents) suggests these organizations present attractive targets due to large customer databases[9][7].

B2B Industrial entities face diverse attack vectors, from DDoS campaigns linked to geopolitical tensions to traditional database breaches. The Santa Barbara Systems attack highlights how geopolitical factors can elevate targeting of defense-related industries[14].

B2G (Government) entities, while showing lower confirmed attack success (only suspected in DGT case), face the potential for massive scale impact affecting entire national populations. The 27+ million records potentially at risk in the DGT incident represents the largest single-organization exposure[16][17].

Success Rate Analysis

- **Confirmed Success Rate**: 91% (11 of 12 incidents)
- **Business Models with 100% Confirmed Success**: B2C Volume/Retail, B2B Industrial, B2C Digital/Fintech
- **Only Suspected/Unconfirmed**: DGT government entity (under investigation)

Regional Threat Landscape Context

The June 2024 incidents occur against a backdrop of escalating cyber threats across LATAM and Spain, with regional attack volumes increasing significantly. Mexico faced 55% of all Latin American cyberattacks in the first half of 2024, while Spain experienced a 35% increase in daily incidents, reaching over 45,000 per day[20][21][19].

This analysis demonstrates that no business archetype enjoys immunity from successful cyberattacks, with threat actors adapting their methods to exploit specific vulnerabilities in each sector. The combination of geopolitical tensions, rapid digital transformation, and insufficient cybersecurity investment has created a perfect storm of vulnerability across the region.