CYJAX

Digital Intelligence
Securing the Future

Strategic Intelligence Report: Latin America and the Caribbean

Introduction

Latin America and the Caribbean together encompass a vast range of territories in Central and South America. The region has historically been marked by economic and political instability, with corruption, military dictatorships and high levels of poverty in many of the countries. However, in more recent years, there have been moves towards democratisation, and interest in what the region has to offer has been increasing throughout the world. In particular, there appears to be a distancing of traditional relationships with the United States and a slant towards China, which has been investing heavily in a range of sectors.

The first part of this paper focuses on the readiness of the region to respond to the increasing number of threats posed by cybercriminals, and on the policies and initiatives which governments are currently implementing. Details of events in a range of countries are also included.

The next section provides a brief overview of cryptocurrency developments and money-laundering concerns.

Finally, there is an assessment of the possibilities for supply chain diversification to Latin America and the Caribbean, particularly in light of Russia's invasion of Ukraine, and China's global ambitions.

The "Gap": Cybersecurity in Latin America and the Caribbean

While internet access continues to improve across Latin America and the Caribbean, there are still marked disparities across the region. According to Statista[1], 90% of people resident in Chile, Uruguay, The Bahamas and Antigua & Barbuda are online in 2023, with the populations of Costa Rica, Argentina, Barbados and the Dominican Republic in second place at 85%. This contrasts sharply with Nicaragua, Guyana and Haiti, where only around 50% of people have access to the internet. Due to sustained investment, mobile connectivity is helping to address the gap, though Venezuela and Ecuador are trailing in this regard.

Governments throughout the region were generally slow in developing national cybersecurity strategies and cybercrime laws compared with some other parts of the world. Brazil, for example, did not publish its first national cybersecurity strategy until 2020. However, in recent years, countries have sought to update their legislative infrastructure in this respect, and have benefitted from expertise derived from international partnerships. The Organization of American States (OAS)[2] has played a prominent part in the evolution of these strategies and policies in Latin America and the Caribbean, working with and advising local administrations on technical training issues and best practices.

It is accepted that there is a real need to focus further on enhancing knowledge and expertise in the region, not only among those working in the cyber sphere in a technical or policy capacity but also in formal educational settings and, crucially, among the general public.

The sharing of expertise and deepening of cooperation among countries in the fight against cyber threats should be encouraged, whether in addressing ransomware attacks carried out by financially-motivated threat actors, cyber-espionage campaigns mounted by state-sponsored groups, or even hacktivist-led operations.

Policy-makers and legal experts in Brazil and Chile, the countries now generally regarded as the regional leaders in the cybersecurity sphere, are particularly well placed to support and advance intelligence initiatives and information-sharing across the region: they can provide guidance on the development of legal infrastructures and encourage continued attention towards enhancing and maintaining up-to-date national cyber strategies. Businesses also have a part to play, especially when it comes to sharing details of threats or successful compromises and data breaches.

In addition, specific laws covering cybercrime are a must, as is the development of international cooperation in countering such illegal activity.

Cyber Threats

According to data collated by Statista[3], Mexico, Brazil and Colombia account for around 90 percent of cyberattacks reported in Latin America.

The major cyber threats include ransomware, phishing, malware, vulnerability exploitation, and DDoS attacks. Attacks may be carried out by state-sponsored threat actors, highly organised criminal gangs, hacktivist collectives or even individuals acting alone.

In the last couple of years, ransomware attacks have become increasingly prevalent globally: this type of malware is currently the preferred choice for cybercriminals, many of whom require little technical ability as they can purchase Ransomware-as-a-Service software on the darknet and also benefit from assistance provided to them with the negotiation of ransom payments and the return of stolen data.

As in other parts of the world, organisations in Latin America and the Caribbean have been hit by ransomware attacks conducted by groups such as Conti, Alphv, LockBit and BlackByte.

Ransomware attacks in the region appear to have increased since the invasion of Ukraine in 2022. This could be driven by the support given by these countries to Kyiv: only Nicaragua, Cuba and Venezuela have failed to condemn Russia's actions. However, while this correlation may be made, it is likely that, as in other parts of the world, a high number of attacks go unreported, and it is by no means certain that the pace of them has gone up any more quickly due to the war.

Latin America and the Caribbean are also targeted by state-sponsored threat actors who mount cyber-espionage campaigns aimed at stealing highly confidential and valuable information, whether from government departments, the military or corporations. North Korean groups such as Lazarus and Kimsuky have been particularly active in this respect, as have a range of Chinese and Russian APTs.

There is no doubt that hacktivist attacks can also lead to serious problems for organisations. While various operations that have taken place over the years have focused predominantly on issues such as government corruption, social inequality, the environment and animal rights, Russia's invasion of Ukraine resulted in new waves of collective cooperation between groups such as Anonymous. In some ways this has even been encouraged by governments. Shortly after the invasion on 24 Feb 2022, the Ukrainian authorities issued a call for hacktivists to gather and launch what can only be described as state-sanctioned attacks on Russian organisations. The appeal was hugely successful: DDoS attacks and data leaks continue to this day. In turn, pro-Russia hacktivist groups formed and launched their own highly damaging campaigns, targeting not only Ukrainian organisations but also those in countries deemed to be supportive of Kyiv. Companies and governments supplying military equipment are at particular risk, and these attacks have increased in 2023. What this demonstrates is that hacktivism remains a real – perhaps a growing – threat, illustrating why it is vital that organisations operating globally pay serious attention to geopolitical developments, whether that be the ongoing war in Ukraine, the increasing tensions between the US and China, or the risk of political instability in Latin American countries such as Mexico, Peru, Ecuador and Bolivia.

The next part of this paper looks at developments in some of the more prominent countries in Latin America and the Caribbean.

Argentina

Argentina is a vast country that is currently implementing extensive economic reforms. Here, as elsewhere in the region, there is a growing risk of cybercrime. DDoS attacks, data leaks, malware, ransomware infections and banking Trojans are all major threats.

Various ransomware attacks have been reported in 2023. The Alphv ransomware group claimed an attack on Akron Maquinas Agricolas (manufacturing); Hector Martinez Sosa y Cia (insurance) appeared on the Qilin ransomware site; the B2B marketplace Export Hub was named as a victim on the CryptNet ransomware site; the Cl0p ransomware operators targeted Global Farm (manufacturing, pharmaceutical); LockBit attacked

Jaureguy (retail, FMCG), Albanesi (energy), and La Segunda (insurance).

Argentina also faces attacks from state-sponsored threat actors. In August 2020, for example, the country was listed as a target in a global campaign against financial institutions orchestrated by the North Korean government's Reconnaissance General Bureau and involving well-known groups such as Lazarus, Bluenoroff and Andariel.

Organisations in the country are also targeted by the Machete group, which again is believed to be state-sponsored, and focuses on high-value targets such as military institutions, embassies, financial organisations, and government agencies. It has been operating since at least 2010.

Argentina's government is committed to the development of a strong ICT industry and laws have been updated to facilitate cloud computing. The telecommunications infrastructure is good, though investment is still needed in rural areas. Internet usage is high.

Argentina signed the Council of Europe's Convention on Cybercrime in 2018 and it entered into force in the same year.

Brazil

Brazil is highly diverse, and home to Latin America's largest population and biggest economy. Payment card fraud is extremely common and facilitated by a variety of methods, including the use of skimming devices attached to ATMs, and compromised point-of-sale (POS) devices. The country is one of the world's top sources of spam, malware and phishing attacks, and a leader in the production of online banking fraud and financial malware.

In 2023 the Alphv ransomware operators have attacked a range of Brazilian organisations, including Grupo Cativa (manufacturing), Lisa Logística, and Fundação Carlos Chagas (professional services). LockBit has claimed attacks on Omega Services (maritime, transportation, aviation) and Grupo Hospitalar Vida's (healthcare), Pharma Gestão, Siqueira Castro(legal (legal), and Primorossi (financial, automotive). Other prominent ransomware groups which have been active include Royal and RansomHouse, which have targeted Ancora- Sistemas de Fixacao (manufacturing, professional services) and the Associação dos Advogados de São Paulo (legal).

Also this year, a new variant of GoatRAT has been identified as utilising an automatic transfer system (ATS) framework to infiltrate Brazilian banks.

Like Argentina and other countries in the region, Brazil has been targeted by state-sponsored North Korean groups, with attacks focusing on government and financial institutions. Chinese threat groups, believed to be working in the interests of the Beijing government, have also launched campaigns aimed at infiltrating organisations active in a range of sectors, including aviation, transportation, insurance and engineering.

As noted above, the Brazilian authorities have been working on improving the country's abilities to deal with cyber threats. In July 2021 a Federal Cyber Incident Management Network was established, aimed at addressing cyber-threats more quickly, as well as enhancing cooperation between federal government bodies.

Brazil signed the Council of Europe's Convention on Cybercrime in 2022 and it entered into force in 2023.

Colombia

Colombia is a major producer of gold, silver and emeralds, and also has substantial reserves of oil and coal. Its main export is petroleum.

Ransomware attacks in 2023 have targeted companies such as Schrader Camargo Colombia (infrastructure), Grupo Vanti (energy), Chemlab, Universidad de la Salle, Keralty (healthcare, insurance) and the Medellin government site. Customer data from Viva Air Colombia was also leaked on a darknet forum.

In May this year the hacktivist group SiegedSec compromised government and energy websites, stealing and leaking data in a campaign named Operation Colombia. The group claimed the attacks were conducted in retaliation for the arrest of a 'fellow hacker'.

Also this year a state-sponsored APT called BlindEagle, a group believed to operate out of South America, has been seen targeting Colombian organisations in the healthcare, financial, law enforcement and government sectors. The group's primary purpose appears to be gaining strategic-level intelligence, allowing the theft of business intelligence or intellectual property.

Colombia was the first Latin American nation to form a national cybersecurity strategy and in 2011 it established specialist government, police and military forces to combat cybercrime. More recently, the government announced the creation of a Digital Committee and a National Cyber Security Agency.

Colombia signed the Council of Europe's Convention on Cybercrime in March 2020 and it entered into force in July that year.

Chile

Chile has one of the highest internet usage rates in Latin American, at over 90 percent. With the wealthiest economy in Latin America, the country is particularly susceptible to the actions of financially-motived cybercriminals

Organisations targeted in 2023 include Apro (retail), Mutual de Seguros de Chile (insurance), Saville Row - Grupo GTD (retail), Cementos Bio-Bio (infrastructure), and DERK (mining).

In 2017 Chile became the first South American country to sign and ratify the Council of Europe's Convention on Cybercrime.

Guyana

The larger nations in the region such as Brazil, Chile, Colombia and Argentina tend to draw global attention and investment for good reason- an abundance of natural resources and general (if somewhat unpredictable) economic growth. However, the country that is currently experiencing the highest increase in GDP- not just in Latin America but in the entire world- is Guyana. Historically one of the poorest countries in the region, its economic prospects are rapidly improving due to revenue from oil production.[4] The discovery of offshore oil reserves in recent years has reignited a long-running border dispute with Venezuela, but is also ensuring that a great deal of investment is being made in the development of infrastructure.

The World Bank and the International Monetary Fund (IMF) estimate that Guyana could see a growth in GDP of almost 100% by the end of 2023, compared with the end-of-the-year figures of 2021.[5]

While the country has yet to attract much attention from cybercriminals, Guyana Goldfields was listed on the Play ransomware site in March 2023. As prosperity increases, more cyberattacks will certainly follow.

Mexico

Mexico suffers from critical levels of crime, particularly related to the drug trade. The homicide rate is also extremely high.

Mexico is rated as the one of countries most heavily targeted by cyberattacks in Latin America. These attacks are frequently directed at the financial sector, and there is a general perception that Mexican cybercriminals are particularly skilled in the development of banking Trojans. Cybercrime is often linked with organised crime, with "traditional" criminal groups increasingly using developments in IT to coordinate activities. Technology has made it easier for these groups to move money across borders and communicate anonymously, and has encouraged involvement in online piracy and counterfeit goods. The sale of stolen data on darknet marketplaces and the production and distribution of child pornography are other lucrative businesses.

Victims of ransomware attacks in the first half of 2023 have included Cydsa (manufacturing), ANCE (professional services); Autlán Metallorum (mining), Grupo Corporacion Control (retail), Mundo Cuervo (hospitality, tourism), Yucatan government, Esperanza Viva Jóvenes de México (NGO), Grupo Floraplant (professional services); Volaris (aviation); Order Express. Avante Textil (manufacturing, retail), and Diavaz (energy), Casa Ley (retail). the Municipal Government of Ciudad Juáre, ITS Servicios (transportation), and Grupo Estrategas EMM (insurance).

Mexico has also been targeted by state-sponsored APTs, including China's Winnti, which focuses primarily on cyber-espionage activities.

Despite having several units tasked with responding to and analysing cyber threats, the legal infrastructure requires further development, and there is a lack of a unified legislative system to combat cybercrime.

Mexico has signed but has not yet ratified the Council of Europe's Convention on Cybercrime.

Costa Rica

Costa Rica is a small country in Central America. It has one of the highest standards of living in the region, though poverty persists within the population.

There have been some notable relatively recent and serious ransomware attacks in Costa Rica. In May 2022 the government declared a national emergency following multiple government bodies being attacked by the Conti ransomware group, which is believed to comprise Russian cybercriminals. Conti published 97% of a 672GB dump containing data stolen from the organisations.

Government and financial institutions have also been targeted by North Korean state-sponsored APTs.

Costa Rica signed the Council of Europe's Convention on Cybercrime in 2017, and it entered into force in 2018.

Cryptocurrency

Several countries in Central America and the Caribbean are notable for their promotion of cryptocurrency.

El Salvador

In June 2021 El Salvador became the first country to adopt Bitcoin as legal tender. Described by PwC as a "bold move", the policy was initiated because some 70% of the population do not have access to a bank account, while the use of mobile phones is extremely high. It was thought there would be major advantages in moving to a monetary system that only required a smartphone app to work.

It is currently unclear how successful this experiment has been. Since the adoption of Bitcoin, the country has been embroiled in political turmoil and there has been an increase in gang-related violence. While there was a predicted rise in revenue from tourism, this has so far been insignificant. The volatility of Bitcoin itself is another factor to be considered.[6]

The Bahamas

In November 2022 more than $600 million was stolen from the cryptocurrency wallets owned by Bahamas-based FTX. The company confirmed that it had been hacked. It later declared bankruptcy.[7] See details here.

FTX founder Sam Bankman-Fried was later arrested and charged with fraud, conspiracy to commit money laundering, and conspiracy to defraud the US and violate campaign finance laws.

Bermuda

Bermuda has also been active in developing the use of cryptocurrency. In April 2023 the country's Premier and Finance Minister confirmed the territory's commitment to digital assets and blockchain technology, and an appropriate legal infrastructure for the regulation of cryptocurrency has been established.[8]

Money-laundering

Several Latin American and Caribbean countries are listed on the European Union’s anti money-laundering blacklist (AML), due to alleged significant tax reporting and financial deficiencies. They currently include the Cayman Islands, Jamaica, Barbados, Trinidad & Tobago and Panama.[9]

The Bahamas was also placed on the list in 2020 but removed after satisfying criteria in 2022.

Panama

In 2016 a whistleblower leaked 11.5 million documents from Mossack Fonseca, a law firm and corporate service provider. The Panama Papers, which were published by various media outlets, contained private financial information about companies and prominent public officials. They showed incidences of Mossack Fonseca shell corporations being used for tax evasion and other fraudulent purposes, including the avoidance of international sanctions.[10]

As noted above, Panama is currently listed on the EU’s AML.

The Cayman Islands

The Cayman Islands, an overseas territory of the United Kingdom, is one of the largest tax havens in the world. A major international financial centre, some 600 banks and trust companies are registered there. The country is currently listed on the EU’s AML.

In addition, in June 2023 the United States Securities and Exchange Commission (SEC) requested that a federal court had issued a temporary restraining order to freeze the US assets of Cayman-based cryptocurrency exchange Binance. It is alleged that the company and its CEO, Changpeng Zhao, operated a “web of deception”, creating separate US entities “as part of an elaborate scheme to evade US federal securities laws”.[11]

Interestingly, the Cayman Islands is reportedly the location of the first-ever sale of property using cryptocurrency.[12] The agent who conducted the transaction using Parallel Limited, a virtual asset service provider (VASP), described it as a “game changer” and a “big evolution” for the Cayman Islands. However, the sales of property to overseas investors and the use of cryptocurrencies are cited by the government as “top concerns” for the risk of money-laundering.

The final section of this paper assesses the prospects for the diversification of supply chains to Latin America and the Caribbean.

Supply Chains

The COVID-19 pandemic provided a salutary lesson in the fragility of global supply chains, leading many organisations to change their practices and embrace digital solutions to control and regulate operations, whether in logistics, manufacturing or ecommerce.

Businesses are also aware of the demands of consumers who want to know the origins of a product, such as where it has been sourced and the supply chain it moved through before reaching them.

Increasing importance, which should not be under-estimated, is being placed on environmental issues such as climate change. Large corporations are responding to these concerns by pledging to deal only with suppliers that adhere to certain environmental standards. The reputational risks to organisations sourcing goods from fragile regions is clear. For example, due to deliberate political decisions made by the government in Brazil, the destruction of the Amazonian rainforest is a particularly controversial topic.

Deforestation is also being seen in other parts of the world, such as in Indonesia. The problem for companies operating in such regions lies in ensuring that each supplier involved in a manufacturing or production chain complies with internationally recognised standards. The Environmental Investigation Agency has cautioned that "some of the companies committing the worst deforestation for palm oil have been entering the supply chains of major international companies with 'no deforestation' policies – including consumer brands such as Colgate-Palmolive, Nestle and Unilever – in a clear breach of those standards".[13]

The European Union has now published a new regulation requiring companies to ensure the palm oil they use has not been produced on land that has been involved in deforestation after 31 December 2020. Such directives are likely to become increasingly common.[14]

Supply chains are also at risk from damaging cyberattacks. There have been several widely reported incidents in recent years. High-profile examples include the Kaseya MSP attack and issues related to Microsoft Exchange Server. The heavily exploited Log4j vulnerability was identified more recently.

Another important attack was seen in the SolarWinds breach of December 2020, when threat actors compromised the company's network, and infected its software with malware designed to target organisations worldwide, particularly in the financial sector.

Russia and China

The invasion of Ukraine has led to a huge number of companies withdrawing operations from Russia. Importantly, it has also resulted in sanctions on Russian organisations and individuals, and a halt to energy exports, Russia's main product.

China also poses problems: there is move away from using it as a manufacturing base due both to concerns over its increasing economic power throughout the world and Beijing's intentions towards Taiwan.

Russia's presence in Latin America and the Caribbean is not new and it currently maintains strong relationships with the governments of Cuba, Venezuela and Nicaragua. It is likely to invest further in the energy and military industries in those countries, and will probably move to attempt to deepen its links with others, such as Bolivia.

China, on the other hand, has only made recent inroads into the region, yet its influence has increased quickly, with huge investments in energy, telecommunications, infrastructure, mining and manufacturing.[15]

From China's point of view investment can only be a positive: it has gained a presence in the same time zone as the US, opening up new markets and supply chains. 20 countries in Latin America and the Caribbean have now signed up to Beijing's Belt and Road Initiative.[16]

Argentina joined in January 2022. The other members are Cuba, Jamaica and six island states in the Caribbean; El Salvador, Costa Rica and Panama in Central America; and Venezuela, Guyana, Suriname, Ecuador, Peru, Bolivia, Chile and Uruguay in South America.

Brazil and Colombia are the only countries in South America that have not yet signed up. Paraguay is not included on any list because it continues to recognise Taiwan – something which is unlikely to change in the near future, given that Paraguay's President-elect Santiago Peña has recently confirmed that his new government will continue to strengthen ties with the island.[17]

Although Colombia has not yet signed up to the Belt and Road Initiative, Chinese companies are heavily involved in some major infrastructure projects in the country, including in the telecommunications and mining sectors. Although the government is aware that its close relationship with the US could be damaged if it chooses to deepen its relationship with Beijing, it is likely that the new president, Gustavo Petro, will be willing to consider such a move if it would be of clear economic benefit to his country.[18]

The prospect of damaging its relationship with its most important partner, the US, is also a factor in the current decision of Mexico's government not to join the Belt and Road Initiative. However, it has important financial and trading partnerships with China which indicate that change could be coming. Cai Wei, Director General of the Department of Latin American and Caribbean Affairs of the Foreign Ministry of China has commented: "Mexico is welcome to participate in the Belt and Road Initiative in fields including finance, 5G, lithium, and electric vehicles to improve supply chain connections between China and Mexico."[19]

These examples are clear illustrations of the main reason for China's determination to expand its activities and investments in Latin America and the Caribbean: the natural resources available for exploitation.

The difficulties involved in diversifying supply chains to countries in Latin America and the Caribbean are rooted in the fact that there are very serious problems in the region. While current global focus is mainly on the actions of Russia in its war with Ukraine, or on China's aggressive economic expansion and its murmurings about invading Taiwan, Latin America is rife with political instability and corruption, along with organised crime fuelled largely by the drug trafficking trade. These issues pose huge problems for companies choosing to diversify supply chains into that region.

As seen above, money-laundering is another major concern. To mitigate against the risk of such activities within supply chains, organisations should implement a range of policies and controls. It goes without saying that vetting a third-party supplier is of crucial importance. Issues of concern can include counterfeit goods being substituted, or prohibited materials being supplied or even sourced contrary to sanctions against companies or individuals.

Cybersecurity policies, part of any due diligence exercise, must include ongoing assessment of policies and practices in place both within the organisation itself and in third-party partners and suppliers, and these should clearly specify immediate disclosure of attacks or data breaches. Regular audits must also be conducted.

Conclusion

Since Cyjax was established in 2012, the company has maintained a keen interest in geopolitics, tracking and tracing cyber events globally while at the same time observing and analysing political, social, economic and environmental issues worldwide. We believe these geopolitical considerations are something that no organisation can afford to ignore, and they should therefore form part of all operational strategies.

China's determination to extend its global reach has already seen huge success in Latin America and the Caribbean, with many countries in the region either having signed up to the Belt and Road Initiative or having embarked on mutually profitable economic partnerships in infrastructure or business projects: this is despite the understandable concerns about Chinese overreach, particularly in the telecommunications sector. This illustrates a move away from the traditional sphere of US influence – something which Washington will not welcome.

Russia, too, hopes to expand its influence in the region, politically and militarily at least, and will continue to offer support to Nicaragua, Cuba, and Venezuela, as well seeking inroads to political and economic partnerships in other countries.

Concerns about both China and Russia have led companies operating globally to consider diversifying their supply chains towards Latin America and the Caribbean. The region certainly has problems and will continue to do so. However, it also offers a tremendous amount in terms of resources and economic opportunities. In this age of digitisation and Artificial Intelligence, countries are taking proactive steps to improve their cybersecurity policies and practices, and this will undoubtedly help them to attract business to the continent.

Endnotes

[1] https://www.statista.com/statistics/726145/latin-america-internet-penetration-countries/

[2] https://www.oas.org/en/sla/iajc/themes_recently_concluded_International_law_State_cyber_operations.asp

[3] https://www.statista.com/topics/7126/cybersecurity-in-latin-america/#topicOverview

[4] https://crsreports.congress.gov/product/pdf/IF/IF11381

[5] https://www.outsourceasia.org/guyana-fastest-growing-economy-in-the-world/

[6] https://beincrypto.com/el-salvadors-bitcoin-experiment-how-is-it-working-out/

[7] https://www.nerdwallet.com/article/investing/ftx-crash

[8] https://freemanlaw.com/cryptocurrency/bermuda-and-cryptocurrency/

[9] https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en#objectives

[10] https://vinciworks.com/blog/a-guide-to-money-laundering-compliance-in-panama/

[11] https://www.aljazeera.com/economy/2023/6/5/us-sec-sues-worlds-largest-crypto-exchange-binance-and-founder

[12] https://caymannewsservice.com/2022/09/cryptocurrency-property-sale-overseen-by-cima/

[13] https://eia-international.org/news/some-of-the-worst-palm-oil-deforesters-in-2022-are-supplying-major-international-companies/

[14] https://environment.ec.europa.eu/topics/forests/deforestation/regulation-deforestation-free-products_en

[15] https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

[16] https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

[17] https://www.aljazeera.com/news/2023/5/5/paraguay-president-elect-says-will-strengthen-ties-with-taiwan

[18] https://www.csis.org/analysis/colombias-relationship-prc

[19] https://www.bjreview.com/World/202303/t20230311_800325153.html

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

CYJAX

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED
IS 676012