nextrends Asia
Ideas & insights from the East

swissnex network locations in APAC hotspots for Cybersecurity

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Japan
在日スイス大使館
Science & Technology Office Tokyo
科学技術部

swissnex network

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

swissnex network
locations in APAC hotspots
for Cybersecurity

Introduction

As more and more aspects of our daily lives, ranging from communication, transportation, financial transactions to medicine, become heavily reliant on computers and the internet, the significance of cybersecurity is also increasing, particularly in the Asia-Pacific (APAC) region where the market is expected to grow most rapidly in the next five years. Interestingly, the swissnex network locations in APAC are exactly the countries named as hotspots for the cybersecurity market.

According to a report[1] by Mordor Intelligence, India has experienced a rapid increase in cybercrime registration, ranking fifth in terms of overall Domain Name System (DNS) hijacks, whereas South Korea is becoming one of the prime targets for cyber-attacks due to the country's increasing number of connected devices and advanced use of mobile devices. Australia is the nation most under attack, with 90% of the Australian companies reporting to have received up to 5'000 threats a day, while India, China, Singapore and Japan are named as emerging markets facing increasing cybersecurity related issues. In the case of China, its sheer size makes a general safety of networks very difficult.

The report forecasts the Asia-Pacific cybersecurity to expand with a 18.3% compound annual growth rate (CAGR) between 2020-2025. This compares to a 14.5% CAGR for the global market.

One reason for the high growth is that the countries are more susceptible to harness technology, to improve lives and livelihood, as the world is about to embrace a new age from information technology with cloud computing, 5G and artificial intelligence (AI) that require a new level of cyber protection. Furthermore, the whole payment system and the huge online shopping business rely on digital transactions which can prove to be critical for hacking. The outbreak of the COVID-19 pandemic will also contribute to the significant growth of cyber-attacks.

Although the above applies to most of the developed countries around the world, the APAC countries are, in general, more adoptive of new technologies, as is the case with deployment of cloud-based services. The CISCO Cybersecurity Series 2019 report[2] found that Asia-Pacific countries tended to have higher percentages of their infrastructures hosted in the cloud rather than on premise. Moreover, In APAC countries, 16% of organisations had between 80-100% cloud-based hosts, compared to 9% globally. In the same survey, 50% felt cloud deployment of cybersecurity solutions offer better data security.

Governments stepping up actions

Strong international partnerships remain key to navigating the increasingly complex cyber terrain. Hence, countries hold bilateral and multilateral dialogues and make collaborative efforts. In 2018, Singapore signed with the Netherlands, the U.S., Australia, Germany,

The CISCO Cybersecurity Series 2019 report found that Asia-Pacific countries tended to have higher percentages of their infrastructures hosted in the cloud rather than on premise.

[1] https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market
[2] https://www.cisco.com/c/dam/global/en_sg/assets/pdfs/cisco-2019-apac-cisco-benchmark-study.pdf

swissnex network
locations in APAC hotspots
for Cybersecurity

Japan and Canada, MOUs that cover cybersecurity cooperation in key areas, such as sharing of information and best practices, cybersecurity training and research, joint cybersecurity exercises with a focus on the protection of Critical Information Infrastructure, and commitment to promote voluntary norms of responsible state behavior in cyberspace.

South Korea in 2019 hosted the Second Inter-Regional Conference on Cyber/ICT Security, cooperating with the Organization for Security and Co-operation in Europe (OSCE) and co-hosted the Warsaw Process Working Group on Cybersecurity with the United States and Poland. Japan has held a series of high-level dialogues with countries such as the U.K., Ukraine, Russia, the U.S., France, EU, India, Israel and more over the past two years. India is a signatory to 39 Mutual Legal Assistance Treaty Agreements, 54 MOUs/ Joint Statements and 10 Cyber Frameworks with various countries. Some of the most prominent ones are with the U.S., Israel and Russia.

Australia is trying to strike a balance between its economic ties with China and its strategic alliance with the United States. More than a simple alignment on U.S. policies towards the People's Republic of China (PRC), Australia's decision to exclude Huawei from 5G infrastructure development can be seen as an expression of concern about Chinese interference in Australia and its growing influence in the region.

In August, Canberra took further steps announcing an additional spending of A$1.66 billion (US$1.19 billion) over the next 10 years to strengthen the cyber defenses of companies and households, in addition to the A$1.35 billion budget announced in June for bolstering the capabilities of its cybersecurity agencies. Broadening the scope of government's protection to businesses is a new approach that will be closely watched.

The Indian government took a similar stance in early summer this year, when it declared it would block more than 100 apps with links to China, including TikTok, citing concerns about national security and data privacy. The move came as a surprise as India had remained neutral in different bilateral and multilateral forums, which is still the official stance of the government.

Meanwhile, China has strictly denied allegations of state involvement in cyberattacks. Still, western states such as Germany and the U.S. have been hesitant to engage in deeper relations with China on cyber security issues and, vice versa, they do not appear in the Chinese strategy as primary partners. Rather, the PRC focuses on collaboration with African and South American Countries, as well as its neighboring countries Japan and the Republic of Korea (ROK). The most recent Trilateral Cyber Policy Consultation among Japan, PRC and ROK was held on November 18, 2019.

Critics have been vocal about the problem, that there is no general policy on blockchain in place yet and the legal basis is limited.

Cross-ministerial lead agencies

The governments are highly committed to cybersecurity and cyber-diplomacy as a safe and secure cyberspace is critical for national security, powering digital economy and finally to protect our digital way of life, as it is said by the Cyber Security Agency (CSA) of Singapore[3].

In terms of organisation, Australia, India, Japan and Singapore have established cross-ministerial lead agencies between late 2014 and early 2015 with the Australian Cyber Centre (ACSC), Indian National Cyber Coordination Centre (NCCC), Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and the Singaporean CSA. The ACSC leads the operational response to cybersecurity incidents, organises national cybersecurity operations and resources, and contributes and provides advice and information to the public, businesses, academic institutions as well as the government about cyberthreats. NICS is the national focal point for coordinating intra-governmental collaboration and promotion of partnerships, linking various governmental bodies with the industry, academia and the public.

While China has an even more integrated system in place, South Korea has maintained a collaborative structure between the multiple governmental agencies[4].

Blockchain use still in the planning

Governments are seeking the use of blockchain for cybersecurity. The Australian Department of Industry, Science, Energy and Resources has released a national Blockchain strategy which aims at capturing the potential value generated via business-related blockchain activities, with a particular focus on supporting global supply chain management systems and tracing.

In India, there is increased focus and research on the use of blockchain technology for cybersecurity. The Institute of Development and Research in Banking Technology (IDRBT) is currently working on one such project to develop a R&D ecosystem for different government departments to foster blockchain technology in the domains of governance, banking & finance and cybersecurity.

As for most other innovative technologies, China also invests heavily in blockchain applications and tries to implement it in its security apparatus.

However, critics have been vocal about the problem, that there is no general policy on blockchain in place yet and the legal basis is limited. Even in Australia, the Digital Transformation Agency released a guide regarding the adoption of distributed ledger technologies in the administration and stressed, among other things, that blockchain is an emerging technology worthy of ongoing observation but in need of standardisation.

Moreover, China's attempt to centralise blockchain under the control of the government is not well received in western countries. Blockchain systems have initially

[3] https://www.csa.gov.sg/

[4] Namely, the Korea Internet and Security Agency (KISA) under the Ministry of Science and ICT, National Cybersecurity Center within the National Intelligence Service, Cyber Bureau within the National Police Agency (NPA) and Information Sharing and Analysis Center for Financial Security Institute, Cyber Command Department of the Ministry of National Defense, and Korean Institute of Criminology. In case of serious cyber intrusions or crimes, the NPA's Cyber Bureau or the Cyber Department of the Prosecutowr's Office takes the lead. The Korean National Computer Emergency Response (KN-CERT) within the National Cyber Security Center of the National Intelligence Service provides technical assistance

been developed to democratise cashflows by emphasising on privacy, avoidance of institutions and anonymous transactions. Taking leverage over this tool would give the state complete insight and control over cashflows and transactions of its users. As China is becoming a more and more cashless society, it would become difficult for individuals to avoid blockchain and hence the government's supervision. This discussion reveals a longstanding controversy on the extent to which privacy should be given up for security, over which China and democratic countries take opposite stances.

In the meantime, Korea and Japan have industry participants moving ahead of the use of blockchain technologies in cybersecurity. KT (formerly Korea Telecom) created GiGA Chain, a 5G network-based blockchain technology to prevent cyberattacks and to increase security for devices connected to the network, by masking the IP address of the devices. Japan's NEC Corp. will offer a service to secure the authenticity of Internet of Thing (IoT) devices using blockchain technologies throughout its life cycle.

nextrends Asia
Ideas & insights from the East

The swissnex Network in Asia collaborates with a broad spectrum of partners related to international research and innovation, supporting them in their outreach and active engagement in the global exchange of knowledge, ideas and talent. swissnex is an initiative of the State Secretariat for Education, Research and Innovation and is part of the Confederation's network abroad managed by the Federal Department of Foreign Affairs. The activities of the swissnex Network in Asia are based on a collaborative approach, relying on public and private partnerships and funding.