IN·SEC·M

MARKET FACT SHEET

South Korea

CREATION DATE 2025 LAST UPDATE DATE 07/2025

INTRODUCTION

South Korea presents a promising market for Canadian cybersecurity companies aiming to expand their footprint due to its rapidly growing economy and increasing focus on digital transformation. The country boasts a highly skilled workforce with a strong foundation in information technology and cybersecurity, providing valuable resources for Canadian firms looking to establish a presence. The South Korean government actively supports the cybersecurity sector through various funding programs and initiatives, which can significantly aid Canadian companies in their expansion efforts.

It is crucial for Canadian companies to become aware of the evolving regulatory landscape governing the cybersecurity market in South Korea. Compliance with these regulations is essential for successful operations in the country.

MAIN DATA

GENERAL DATA[1]	
Area	› Located in East Asia › 100,363 square kilometers
Capital	Seoul
Time Zone and Time Difference with Ottawa	Korea Standard Time (KST) (UTC +09:00) (13 hours ahead of Toronto)
Languages	Korean
Population	51.8 million (2024)
Religions	Christianity and Buddhism (Majority)
Major Holidays[2]	› New Year's Day (January 1) › Korean New Year (Seollal) (Moveable feast, based on the Lunar calendar) › Independence Movement Day (March 1) › Buddha's Birthday (Moveable feast, based on the Lunar calendar) › Children's Day (May 5) › Memorial Day (June 6) › National Liberation Day (August 15) › Chuseok (Korean Thanksgiving) (Moveable feast, based on the Lunar calendar) › National Foundation Day (October 3) › Hangeul Day (October 9) › Christmas Day (December 25)
Typical Working Hours	› Standard working 40 hours › 5-day workweek, Monday to Friday
Entry Requirements	› **Passport Validity**: Passport must be valid for at least the expected duration of your stay. › **Visa Requirements for Canadians[3]**: Canadians do not need a tourist or business visa, and they are exempt from the K-ETA requirement until December 31, 2025. Student and working visas must be obtained before arrival, and visa status cannot be changed within South Korea.

1. South Korea country profile - BBC News
2. Public Holidays : VISITKOREA
3. Travel advice and advisories for South Korea

Tax Treaties	The Canada-South Korea Tax Treaty was signed on September 5, 2006, and came into effect on January 9, 2007. The treaty helps prevent double taxation, facilitates trade and investment, and includes provisions for tax dispute resolution. It also establishes withholding tax limits: 5% on dividends between affiliated companies, 15% on other dividends, 10% on interest, and 10% on royalties.[4]
POLITICAL DATA[5]	
Type of Political System	South Korea is a unitary presidential republic. The executive branch consists of the President as the head of state and government, who is elected by popular vote for a single five-year term. The President appoints the Prime Minister (subject to National Assembly approval) and oversees the Council of Ministers. The legislative branch is a unicameral system with the National Assembly, which has 300 seats. Members are elected through a mixed system: 253 members are elected in single-member districts by a simple majority vote, while 47 members are elected by proportional representation. Legislators serve four-year terms.
Leaders	Lee Jae-Myung is a South Korean politician and lawyer who is the 14th president of South Korea. A member of the Democratic Party of Korea, he held office as the party's leader from 2022 to 2025 and represented Gyeyang B in the National Assembly from 2022 to 2025.
Regime Stability	In early 2025, Korea faced political uncertainty due to the impeachment of President Yoon Suk Yeol. Since the election and inauguration of President Lee Jae-Myung, regime stability has improved.
ECONOMIC DATA (MAIN ECONOMIC INDICATORS)	
Economic Situation	**Entire economy:** › USD $1.71 trillion GDP (2023)[6] › The potential economic value of South Korea's digital transformation is estimated at KRW 281 trillion (USD 236 billion) annually by 2030 (2021)[7] › South Korea is set to invest 1.1 trillion won ($827.1 million USD) towards the cybersecurity sector by 2027.[8]
Financial Situation	› **Currency:** South Korean Won (KRW) › 1 CAD equals approximately 1,020 South Korean Won (as of March 2025) › **Inflation Rate**: 1.9% (estimated for 2025)[9]
Economic Policies Relating to IT Sector	**National Cybersecurity Strategy [10] [11]** South Korea's National Cybersecurity Strategy (2019) marked a shift from a traditional defensive approach to a more proactive, offensive stance in cybersecurity. The updated version in 2024, developed by 14 government ministries including the Ministry of Science and ICT and the National Intelligence Service, outlines 100 action tasks aligned with five key strategic priorities: strengthening offensive cyber defense, enhancing global cooperation, improving the resilience of critical infrastructure, securing a competitive edge in emerging technologies, and strengthening the operational foundations across sectors. Notably, the plan includes measures for preemptive cyber defense and international collaboration to build a secure and peaceful cyberspace. The South Korean government also aims to foster a strong cybersecurity ecosystem through public-private partnerships and the advancement of key technologies like AI and cloud computing.
Digital Transformation › Internet penetration rate › Digital literacy ranking › Cybersecurity investments › Other relevant data	› **Internet penetration Rate:** 97% (2023)[12] › **Digital literacy ranking**: South Korea has an exceptional digital literacy rate, demonstrated by 97.1% smartphone penetration, including 90% adoption among individuals aged 60 and above.[13] › **Cybersecurity investments**: #3 according to the Cyber Defense Index 2022/23 published by MIT Technology Review[14] › **Other relevant data**: N/A

4. Convention Between Canada and the Republic of Korea - Canada.ca
5. South Korea | History, Map, Flag, Capital, Population, President, & Facts | Britannica
6. GDP (current US$) - Korea, Rep. | Data
7. Unlocking South Korea's KRW281-trillion digital opportunity by 2030 - Access Partnership
8. S.Korean gov't to invest $827 mn in cyber security sector by 2027 - KED Global
9. South Korea Inflation Rate
10. Korea - Digital Economy
11. South Korea's 2024 Cyber Strategy: A Primer | Strategic Technologies Blog | CSIS
12. Individuals using the Internet (% of population) | Data
13. Digital literacy among Korean older adults: A scoping review of quantitative studies - PMC
14. The Cyber Defense Index 2022/23 | MIT Technology Review

POLITICAL AGREEMENTS AND RELATIONS WITH CANADA	
Political Agreements and Relations with Canada	› Canada and South Korea maintain strong diplomatic relations with regular high-level exchanges. › Both countries are members of the United Nations and share common interests in regional security and global stability. › They signed the Canada-South Korea Free Trade Agreement (CKFTA) in 2014, promoting economic cooperation.[15] › South Korea is a key partner in the Asia-Pacific region for Canada's foreign policy, with cooperation in trade, peacekeeping, and education. › Canada is the host of G7 Summit in 2025, and had invited the newly elected President Lee Jae-Myeung to attend.

MAJOR PLAYERS

Government

Ministry of Science and ICT (MSIT) [16]
This ministry is responsible for the protection of private sector information security, setting policies, and overseeing cybersecurity efforts in telecommunications and technology industries

National Intelligence Service (NIS) [17]
NIS plays a significant role in securing national e-government systems and preventing leaks of sensitive state information. The National Cyber Security Center under NIS is responsible for coordinating national cybersecurity policies, detecting cyber threats, and supporting response efforts

Private Sector

AhnLab[18]
AhnLab is a leading cybersecurity solutions provider in South Korea, offering services such as antivirus software, endpoint protection, and network security. The company is best known for its V3 antivirus product and provides robust security solutions to both the public and private sectors.

Penta Security Systems[19]
Penta Security is a prominent South Korean company that specializes in web application firewalls, data encryption, and identity management solutions. The company is recognized for products like WAPPLES and DBCrypt, designed to protect businesses' digital infrastructures.

SK Infosec [20]
SK Infosec, part of the SK Group, is a leading provider of network security, cloud security, and managed security services. The company focuses on securing critical infrastructures and offers comprehensive cybersecurity services for large enterprises.

Est Security [21]
Est Security is known for creating the ALYac antivirus software, and it offers endpoint protection, threat intelligence, and security consulting services. The company is well-regarded for its innovative approaches to malware protection.

Secui [22]
Secui is a leading South Korean cybersecurity company specializing in advanced network security technologies. Established in 2000, Secui has built a reputation as Korea's top security expert group, recognized for its technical excellence and innovation.

15. Individuals using the Internet (% of population) | Data
16. Digital literacy among Korean older adults: A scoping review of quantitative studies - PMC
17. The Cyber Defense Index 2022/23 | MIT Technology Review
18. AhnLab
19. Home | Penta Security Inc.
20. Cybersecurity | SK shieldus
21. ESTsecurity Corp.
22. Overview of Company - SECUI | COMPANY INFORMATION | SECUI

IGLOO Security [23]
IGLOO Corporation is a South Korean cybersecurity company, established in 1999 and headquartered in Seoul. Formerly known as IGLOO Security, the company has played a leading role in advancing the information security market by delivering a broad range of cybersecurity solutions and services to both domestic and international clients.

WINS TECHNET [24]
WINS Technet, commonly known as WINS, is a leading South Korean cybersecurity company specializing in network security solutions. Founded in 2000 and headquartered in Seoul, WINS provides advanced security technologies and services to protect critical network infrastructure for enterprises, telecommunications providers, and government organizations.

Fasoo [25]
Fasoo is a South Korean cybersecurity company that provides unstructured data security, data governance, and AI-powered enterprise content platforms to help organizations discover, classify, protect, and manage critical information assets while boosting productivity.

Academic

Korea Advanced Institute of Science and Technology (KAIST) [26]
KAIST is highly recognized for its research and innovation in the field of cybersecurity, offering advanced degrees and specializations in computer science, including cybersecurity.

Seoul National University (SNU) [27]
Known for its computer science and engineering department, SNU offers strong research opportunities in cybersecurity, particularly in areas like network security and cryptography.

POSTECH (Pohang University of Science and Technology) [28]
POSTECH provides specialized courses and research opportunities in cybersecurity, with a focus on scientific and technological aspects.

Sungkyunkwan University (SKKU) [29]
SKKU offers graduate programs in software and computer engineering, with options to focus on cybersecurity-related courses.

Hanyang University [30]
With its robust computer science program, Hanyang University provides opportunities to focus on cybersecurity through advanced coursework and research projects.

Association

National Cyber Security Laboratory (NCSL) [31]
This association, under the National Assembly Secretariat, focuses on research and providing legislative support for cybersecurity laws. It collaborates with lawmakers to help shape crucial cybersecurity legislation, such as the Framework Act on National Cybersecurity.

Korea Internet Security Agency (KISA) [32]
KISA is an essential government-backed organization that provides cybersecurity measures and services. It promotes industry collaboration, supports cybersecurity research, and engages in international partnerships to strengthen South Korea's cybersecurity infrastructure.

23. Overview - Security & Intelligence IGLOO Corporation
24. About WINS Technet | WINS Technet
25. AI-Ready Data Security and Privacy | Fasoo
26. KAIST
27. Seoul National University
28. POSTECH
29. Sungkyunkwan University
30. Home - Hanyang University
31. New cybersecurity association aims to bolster South Korea's legislative framework » The Readable
32. KISA

INTERNATIONAL COMPETITION

Research on cybersecurity-related foreign direct investment projects in South Korea since 2021 identified only one project originating from the United States. Claroty[33], the leading security company for cyber-physical systems (CPS) across industrial, healthcare, and commercial environments, has established a regional headquarters in South Korea to strengthen its penetration into the local market.

STRENGTHS AND WEAKNESS OF CYBER SECURITY ECOSYSTEM

STRENGTHS

- Strong Government **Support: The South** Korean government has made cybersecurity a national priority, with continuous efforts to strengthen cybersecurity strategies, regulations, and investments in the sector. This includes support through KISA (Korean Internet Security Agency) and other governmental initiatives.
- **Advanced Technological Infrastructure**: South Korea boasts one of the fastest and most sophisticated digital infrastructures globally, making it a leader in tech-driven cybersecurity solutions.
- **Industry Collaboration**: Strong collaborations between government, industry players, and academic institutions, such as those with KAIST and POSTECH, foster innovation and ensure research and development efforts are effectively supported.
- **High Demand for Cybersecurity Solutions**: Due to its robust IT infrastructure, South Korea faces high cybersecurity threats, driving an increasing demand for advanced cybersecurity solutions, especially from large enterprises and government entities.
- **Global Cybersecurity Reputation**: The country is known for its proactive stance on cybersecurity and regularly hosts cybersecurity events, contributing to its reputation as a regional hub for cybersecurity innovation.

WEAKNESS

- **Cybersecurity Threats**: Despite advanced defenses, South Korea remains a frequent target of cyberattacks, particularly from state-sponsored groups. The high frequency of attacks strains resources and poses challenges for maintaining national cybersecurity.
- **Limited Focus on Smaller Enterprises**: While large organizations benefit from strong cybersecurity, SMEs (Small and Medium Enterprises) still face challenges due to limited resources and cybersecurity awareness.
- **Dependency on Foreign Solutions**: South Korea's cybersecurity sector heavily relies on foreign technology providers for certain advanced solutions. This creates vulnerabilities, especially in critical infrastructure sectors.
- **Complex Regulatory Landscape**: Despite significant governmental focus, navigating the complex cybersecurity regulations and funding mechanisms in South Korea can be challenging for both domestic and foreign companies.

33. Claroty launches full-scale entry into South Korea - Orange Magazine

MAIN NEEDS/END CUSTOMERS/MAJOR PROJECTS IN PROGRESS TO COME

South Korea's cybersecurity market is driven by the need to safeguard its advanced digital infrastructure, as the country faces frequent cyber threats. The growing adoption of cloud computing, smart cities, and e-commerce further heightens the demand for cybersecurity solutions, particularly in sectors such as finance, healthcare, and telecommunications. The ongoing risks are prompting major enterprises and government agencies to seek more robust cyber defense systems.

Key projects include government-led initiatives under the National Cybersecurity Strategy, focusing on enhancing regulations and securing critical infrastructure. The country is also strengthening private sector cybersecurity with investments in AI, blockchain, and cloud technologies. These efforts aim to build resilience and drive demand for advanced cybersecurity solutions.

MARKET PENETRATION: OPTIMAL APPROACH AND OTHER CONSIDERATIONS

To successfully penetrate the South Korean cybersecurity market, foreign companies, especially those from Canada, should focus on building strategic partnerships with local firms. Collaborating with South Korean technology providers, academic institutions, and government agencies such as KISA (Korean Internet Security Agency) will help establish credibility and facilitate market entry. South Korea's emphasis on collaboration between the public and private sectors, along with its strong cybersecurity laws and regulations, offers ample opportunities for international firms to participate in national cybersecurity defense projects.

Additionally, Canadian firms should engage in government-led cybersecurity initiatives like the National Cybersecurity Strategy, which emphasizes securing critical infrastructure and advancing cybersecurity technologies. Participating in public-private partnerships or contributing to cybersecurity legislation can provide visibility and influence within the market. Given the increasing demand for cybersecurity across industries, especially with South Korea's rapid technological advancements, adopting a localized approach will be key to gaining traction.

EVENTS

› **Zer0con**	April 10-11, 2025
› **International Security Conference (ISEC)**	August 26-27, 2025
› **International Security Exhibition & Conference (SECON)**	March 18-20, 2026

BUSINESS ENVIRONMENT AND PRACTICAL ADVICE

For Canadian firms looking to enter the South Korean cybersecurity market, understanding the local business environment is crucial. South Korea has a strong cybersecurity infrastructure, with the government placing a high emphasis on national security, including through the Korean Internet Security Agency (KISA). To navigate this, forming local partnerships with industry associations such as KISA and participating in government-led initiatives like the National Cybersecurity Strategy will provide valuable insights and networking opportunities.

Compliance with local regulations, such as South Korea's Personal Information Protection Act (PIPA) and other cybersecurity-related laws, is essential for successful market entry. Canadian companies should also align with South Korea's growing focus on cybersecurity education and innovation, collaborating with local academic institutions like KAIST and POSTECH to stay ahead of technological trends. Engaging in public-private partnerships, which are common in South Korea, can offer Canadian firms the chance to enhance their presence and influence policy development.

Useful Contacts

The Embassy of Canada to South Korea
seoul@international.gc.ca

In-Sec-M
Lysanne Picard,
lysanne.picard@insecm.ca
Nicolas Duguay,
nicolas.duguay@insecm.ca

Find Out More

- Please see footnotes

In-Sec-M's Mission Report 2025