Department for
International Trade

MADE IN THE UK
SOLD TO THE WORLD

SOUTH KOREAN MARKET INTELLIGENCE REPORT 2022

INFO SECURITY

Department for
International Trade

The UK’s Department for International Trade (DIT) helps businesses export, drives inward and outward investment, negotiates market access and trade deals, and champions free trade.

We are an international economic department, responsible for:

- supporting and encouraging UK businesses to drive sustainable international growth
- ensuring the UK remains a leading destination for international investment and maintains its number one position for international investment stock in Europe
- opening markets, building a trade framework with new and existing partners which is free and fair
- using trade and investment to underpin the government’s agenda for a Global Britain and its ambitions for prosperity, stability and security worldwide.

About Intralink

This market intelligence report has been developed by Intralink.

Intralink is an international business development and innovation consultancy specialising in East Asia. The company's mission is to make commercial success in new global markets fast, easy and cost effective.

Intralink has 120 multilingual employees, a track record of over 30 years, and offices in South Korea, China, Japan, Taiwan, Singapore, the UK, the United States, Israel, France, Poland and Australia.

The company helps western businesses to expand in East Asia, Asian companies to collaborate with western innovators, and governments from around the world to grow their exports and attract foreign direct investment.

Intralink does not just develop its clients' strategies but plays a hands-on role in building their businesses. Its teams in Asia – immersed in the cultures and business practices of their local markets – identify opportunities, negotiate deals, and generate revenues. And when the client is ready, they will help set up an in-country presence through a local subsidiary or partnership.

Intralink's clients range from technology start-ups and SMEs to multi-national corporations and economic development agencies from Europe, North America and Asia. The company's specialist teams – in sectors such as energy, mobility and healthcare – are working with leading-edge, enabling technologies to help its clients develop and deliver solutions for the big challenges of our time.

www.intralinkgroup.com

Intralink

CONTENTS

Table of Figures

Table of Tables

01 INTRODUCTION

South Korea (Korea) has a technologically advanced, export-driven economy and although it is one of the most connected nations on earth, aspects of its infrastructure have proven to be vulnerable to cyber-attacks. The government and private industry have heightened their security protocols in recent years after several high-profile hacking cases and the local InfoSec solution market is showing strong growth potential. The market has grown rapidly over the past decade, but it further accelerated in 2020 as Digital Transformation became an even more pressing matter due to the COVID-19 pandemic.

The Korean InfoSec market reached GBP 7.4bn in value in 2020, a 6.4% increase from 2019. According to Korea Information Security Industry Association (KISA)'s research on information security practices, Korean companies allocated on average 61.8% of the total IT budget for information security in 2020, a 29.5% increase from the previous year. This, along with a rapid increase in the number of Korean companies and organisations appointing Chief Information and Security Officers (CISO) in recent years, shows that information security is moving up the agenda.

Local players such as SK Shieldus (a merger between SK Infosec and ADT Cap, currently the biggest security solution provider in the country) and AhnLab are major providers of InfoSec solutions along with well-established global players. In recent years, fintech and cyber security start-ups have been addressing the growing market demand for cloud services, Digital Rights Management (DRM), Data Loss Prevention (DLP), Operation Technology (OT), and Artificial Intelligence (AI) solutions with a focus on the growing need for remote services. System integrators and security consultancies are also part of the ecosystem and often act as value-added resellers of local and overseas products.

The Korean InfoSec market can be challenging but also rewarding to overseas solution providers. Finding a niche within the information security sector and leveraging a local partner's experience in manoeuvring through the local business culture and regulations is one recipe for success. There is a growing pool of local InfoSec start-ups challenging the status quo which could emerge as a dominant force in the coming years, making the market more competitive and crowded but for now, there is still plenty of opportunity for UK companies to establish a presence in the local market. Further, because the UK's expertise in this field are widely acknowledged in Korea, those companies should be met with a warm reception.

For UK companies in the sector, increasing budgets allocated to information security, strengthening security policies, relatively weak local innovation to-date and increasing moves towards deregulation in the area all combine to make Korea a potentially attractive market. Opportunity areas include finance (internet banking, digital payments, biometric identification, fraud detection, blockchain and the public sector), cyber-terrorism prevention, encryption, distributed denial-of-service (DDoS), ransomware and other cyber-threat detection, InfoSec consulting, as well as general data encryption and encryption software for e-commerce.

02

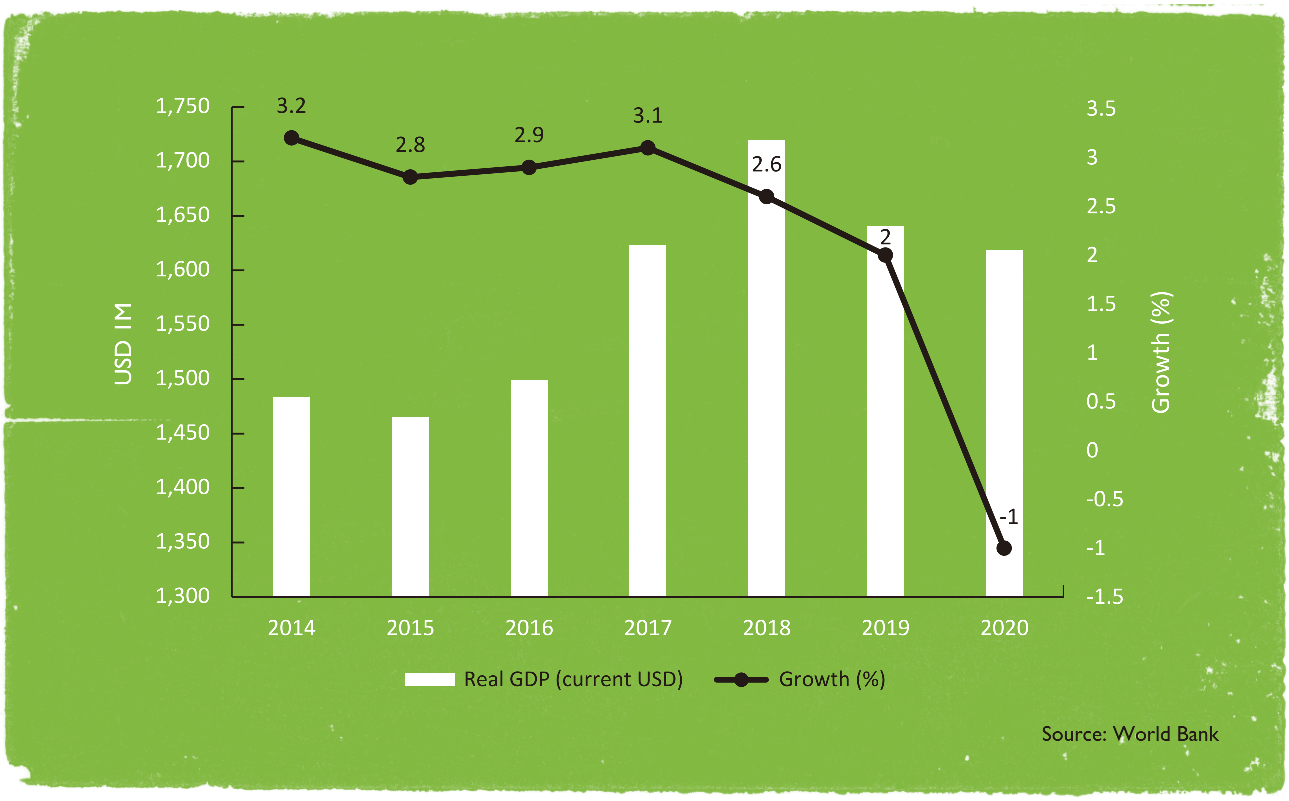
KOREA: AN OVERVIEW

In the space of just 60 years, Korea has transitioned from an agricultural economy to one driven by high value industries such as automotive, shipbuilding and advanced manufacturing. Perhaps most remarkable of all is the country's success in the area of information communications technology where the country has become world class in terms of semiconductor, consumer electronics and ICT infrastructure.

With a population of 51 million people, Korea boasts the 10th largest economy in the world, a GDP of £1.21 trillion ($1.63 trillion) in 2020 and a per capita GDP of £23,300 ($31,500) that same year. Whilst no longer experiencing the dizzying growth rates that characterised its early growth phase in the second half of the twentieth century, Korea has maintained strong growth for a developed economy of close to 3% in the years prior to the outbreak of the COVID-19 pandemic.

Total trade (exports and imports) between the UK and Korea was £13bn in the four quarters to the end of Q2 2021, an increase of 6.1% or £749m over the preceeding 12-month period. Of this, UK exports to Korea totalled £7.5bn while its imports from Korea came to £5.5bn. Korea is the UK's 22nd largest trading partner and accounts for 1.1% of total UK trade. The UK and Korea signed a continuity free trade agreement in 2019 which largely replicated the EU-Korea agreement.

Figure 1: GDP and Growth Rates (2014-2020)



Source: World Bank

03

THE INFORMATION SECURITY MARKET IN KOREA

Key Points

- The Korean InfoSec market stood at GBP 7.4bn in 2020, a 6.4% year-on-year increase
- Recent years have seen an increasing number of attacks originating from North Korea and China
- Key domestic players include SK Shieldus, AhnLab, Secui, WINS and Penta Security
- Opportunities exists to supply both to government initiatives against international hacking, to financial institutions seeking secure internet transactions and to provide secure cloud services

According to a survey conducted by the Ministry of Science and ICT (MSIT), in 2020 there were 1,283 information security enterprises in Korea, up from 1,094 in 2019. The number of personnel involved in the InfoSec industry was over 54,000 in 2020 with an additional 8,000 new employees hired in the sector that year. This growth is expected to continue as companies in Korea acknowledge the importance of InfoSec. As of 2020, 69.5% of Korean enterprises were using InfoSec services, a 27% increase from the previous year. The intellectual property rights acquired or ready for registration related to information security totalled 3,169 cases in 2020 – 2,909 acquired intellectual property rights and 260 intellectual property rights that are pending.

InfoSec industry revenue has been growing 8.7% year-on-year. Factors that are driving such growth include reform of government laws and regulations, strengthening security policies, increased investments by the government and corporates, increased awareness from recent security breaches and a willingness to expand to overseas markets. By demand, network security systems recorded the highest revenue, followed by security management systems, network security systems, and security consulting.

As the market grew domestically, so did InfoSec solution exports. In 2020, export figures reached GBP 1.2bn, an 8.8% increase from 2019. Since 2014, the average yearly growth rate of the InfoSec export market has been 4%. Among local InfoSec organisations, 168 enterprises invested on average GBP 1.3bn in R&D – approximately 15% of annual revenue across the industry.

Table 1: Sales Forecast for InfoSec and Security Sector

Year	Infosec	Security	Total
2018	1.93bn	4.41bn	6.34bn
2019	2.2bn	4.6bn	6.8bn
2020	2.4bn	4.96bn	7.36bn

Source: KISA; Unit: GBP

Table 2: Number of Domestic InfoSec Industry Companies

Year	Infosec	Security	Total
2020	531	752	1,283
2019	473	621	1,094
2018	464	549	1,013
2017	332	565	897
2016	311	553	864

Source: Survey for Information Security Industry in Korea: Year 2021

While Korean security solution providers outpace information security, such a trend is somewhat backwards compared to the global market standard. According to Gartner forecast in 2021, the global InfoSec market is expected to reach GBP 112.1bn in revenue while the security solutions and services market will mark GBP 54bn. This gap is expected to widen as the demand for remote workplace enabling software and cloud security services grows rapidly.

Industry Insider's Thoughts

Korea is a manufacturing-based economy. Although the industry is looking to integrate smart factory solutions in its factories, there isn't enough investment into it. In addition, Korea lacks acknowledgement to pay for software services. Many small-medium sized corporates use free software intended to be released for the general public.

Anonymous in the interview with the Digital Daily on Information Security

Table 3: Worldwide Security Spending by Segment 2020-2021

Segment	2020	2021	Growth (%)
Application Security	2,533.1	2,840.9	12.2
Cloud Security	452.2	639.2	41.2
Data Security	2,265.6	2,663.8	17.5
Identify Access Management	9,147.4	10,576.9	15.6
Infrastructure Protection	15,551.1	18,166.3	16.8
Network Security Equipment	11,875.8	12,935.2	8.9
Other Information Security Software	1,752.6	1,920.5	9.6
Security Services	49,453.2	55,097.7	11.4
Consumer Security Software	4,945.3	5,312.4	7.4
Total	97,976.2	110,152.9	133,776

Source: Gartner (May 2021); Unit: million GBP

CYBER THREATS IN KOREA

With ever expanding device connectivity comes an increasing need for security measures to protect data. In 2020, hackers were targeting VPNs and Microsoft Exchange to access companies' networks as well as exploit vulnerabilities in remote code access. Ransomware and DDoS attacks were also popular hacking methods. A total of 6,034 cyber-attacks were reported last year and most used malicious code to launch the attack. In addition, the number of civilian hackers attacking other citizens has also grown. According to the National Office of Investigation of the National Police Agency, there were 1,075 reported cases of cybercrime from March to October 2021. Hacking of personal data constituted 75.3% of all cases.

In addition, North Korea is posing an ever-increasing risk. Due to COVID-19, it was impossible for North Korea to maintain annual revenue typically brought into the country through its limited trade networks. As a countermeasure, the country appears to be attacking banks and cryptocurrency exchange centres around the world to extort funds from these institutions.

Closer Look

Korea is also experiencing security threats of domestic origin. In November 2021, a domestic hacker infiltrated thousands of smart wall pads installed at apartments around Korea. The wall pads have been actively introduced as part of the Korean government's Smart Home IoT Initiative. A local hacker group leaked videos recorded using the devices and is still circulating them on the dark web and making profit via cryptocurrency. The Korean National Police Agency's cyber police have initiated an inquiry into the degree of harm, and the government has mandated that the wall pad network of homes be separated. Unfortunately, this will only be applied to newly built apartments.

Due in part to its vulnerable geopolitical situation, South Korea has experienced an increasing number of attacks believed to originate from North Korea and China, making the information security issue not only a threat to everyday users and businesses, but also to the state. In June 2021, the Korea Atomic Energy Research Institute (KAERI) was exposed to 12 days of hacking attempts from North Korea, exposing critical research documents. The IP phishing attacks were targeted at pharmaceutical companies, hospitals, and high-ranking government officials. The Bank of Korea came under 1,209 attacks in 2021 alone, 27 times higher than in 2016 (44 attacks). In the same year Korea as a whole experienced hacking attacks originating from the US (814), Russia (765 times), Brazil (747 times), and China (738 times).

Although cyber security is recognised by the Korean government as a matter of national security, Korean companies still trail behind in InfoSec when compared to other technologically mature nations. To narrow this gap, the government and industry joined forces to strengthen the regulatory and technological framework against international hacking. At the same time, financial institutions and other commercial sectors are engaged in an effort to make internet-based services safe and convenient for everyday users. The rising number of both external and internal hacking and cyber threats, which local competitors are struggling to contain, along with increased spending on IT security presents an opportune moment for UK companies to enter the market.

INFORMATION SECURITY POLICY

The Korean government has been actively working to increase the competitiveness of domestic firms in the InfoSec industry and aims to have Korean companies grow their share of the domestic market. This policy was reflected in the Digital New Deal policy announced after the outbreak of the COVID-19 pandemic. The Digital New Deal is an inter-government fund established to facilitate national innovation projects with a focus on job creation and the transition to a digital economy.

The initiative is being led by the MSIT and the allocated budget is set to reach GBP 37bn. Its key objectives are to promote the K-cybersecurity strategy to respond to the paradigm shift in the InfoSec sector and build a safer digital nation. In addition, the government has set a roadmap to invest GBP 426m by 2023 to raise Korea's cybersecurity level and become the fifth most secure nation in the world while decreasing the private sector cyber incident rate to less than 1.5% and supporting the growth of the InfoSec market. Next to measures stimulating the growth of sectors connected to InfoSec, another major role of the government is enacting regulations to enhance personal data protection and data security.

EVOLUTION OF THE REGULATORY ENVIRONMENT

The Korean information security industry began to emerge in the mid-1990s. The Korea Information Security Industry Association (KISIA) – the first non-government organisation with a mandate to impose structure on the industry – was formed in 1998. Since the early 2000s, the industry has seen steady growth resulting in the creation of the Information Security Management System (ISMS), a comprehensive system for establishing, managing and operating organisational IT infrastructures to safeguard key information. To enhance the security environment, Korea's National Intelligence Service (NIS) handles the public sector, and MSIT oversees the private sector.

However, these government agencies mainly focus on responding to malicious activities and developing practical countermeasures to incoming threats rather than developing a comprehensive national cybersecurity policy. In the past decade, accidents created by low information security measures have raised awareness among lawmakers, the industry, and the public of the need for the government to take proactive measures to address the threat.

Designating and Registering Chief Information Security Officer

According to the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., communication and information providers must have a designated Chief Information Security Officer (CISO) at an executive level, and as of June 2019 CISOs are banned from working at dual roles, such as Chief Information Officer (CIO). The revision was implemented to emphasize the importance of the fact that CISOs should place their undivided attention on ensuring the security of the company and its clients' information. By the end of 2020, 24,000 companies were reported to have a designated CISO.

Korea's Information Security Management System

The Korean government introduced a certification system called Information Security Management System (ISMS) in 2001. It is a comprehensive system for establishing, managing and operating organisational IT infrastructure to protect key information assets against external threats. Since its introduction, most public institutions have been required to use ISMS-certified security solutions. The requirement also extends to IT infrastructure companies such as internet service and data centre providers, and information and communication service providers of a certain size.

As a member of the World Trade Organization (WTO) and a signatory to its Government Procurement Agreement (GPA), Korea is obliged to emphasize transparency and non-discrimination against foreign companies. However, Korea is exempt from the GPA rules regarding procurement related to national security and defence. The official certification system often acts as a barrier to foreign companies. Even though there is no evidence that the government-led ISMS certification system offers any additional layer of security compared to global standards, global norms such as ISO 27001 and PCI-DSS are not valid in Korea. In addition, ISMS certification usually takes about five to eight months to obtain, and the cost can reach GBP 9,000. In 2019, the Korean government created ISMS-P, a joint certificate to diminish redundancy between ISMS and the Personal Information Management System (PIMS).

Industry Insider's Thoughts

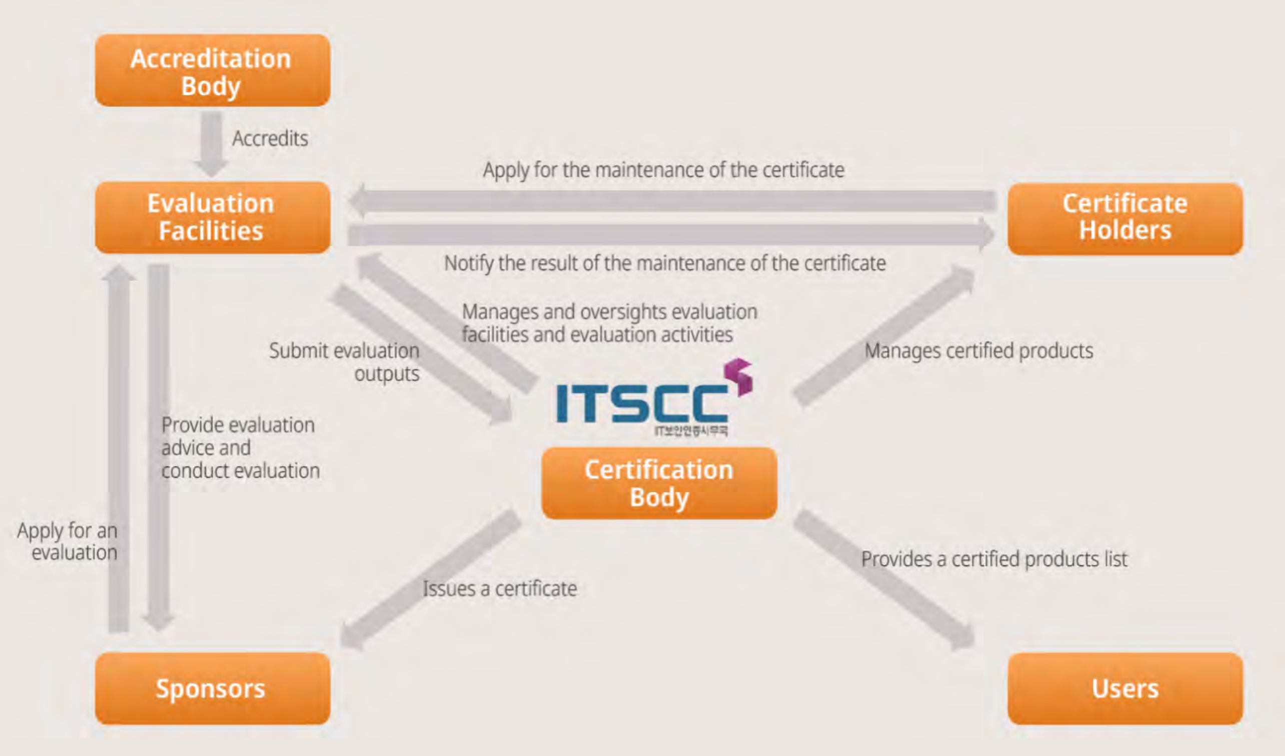
We cannot expect the government and conservative regulations to keep pace with the rapidly changing security market and the technology that develops day by day.

National Information Protection White Paper - Korea Internet & Security Agency

Information Security Product's Evaluation and Certification System

In Korea, there are three organisations that oversee the evaluation and certification system for information security products. The roles and responsibilities include policy, certification and evaluation. With regards to the policy, the MSIT defines and establishes policies, standards, and regulations for information security products and manages organizations that certify these products. The IT Security Certification Centre of the National Security Research Institute (NSRI) serves as the certification organisation and issues reports and confirmation for security validity certification and designates evaluation institutions. As the next step, evaluation organisations such as KISA, Korea System Assurance (KoSyAs), Korea Security Evaluation Laboratory (KSEL), Telecommunications Technology Association (TTA), Korea Information Security Technology (KOIST) and Korea Testing Certification Institute (KTC) are tasked with evaluating information security products.

Figure 2: Product Evaluation and Certification Process


Accreditation Body
Accredits
Evaluation Facilities
Apply for the maintenance of the certificate
Certificate Holders
Notify the result of the maintenance of the certificate
Manages and oversights evaluation facilities and evaluation activities
Submit evaluation outputs
Manages certified products
ITSCC
IT보안인증사무국
Provide evaluation advice and conduct evaluation
Certification Body
Apply for an evaluation
Issues a certificate
Provides a certified products list
Sponsors
Users

Source: KISA

LEADING DOMESTIC PLAYERS

Korea has several large players in the InfoSec industry that supply primarily to the local market. The largest information security company in Korea is SK Shieldus – an affiliate of the SK Group established through an M&A between SK InfoSec and ADT Caps. SK InfoSec specialises in enterprise-grade security solutions including server protection and security platforms, while prior to the merger ADT Caps had specialised in security consulting as well as designing and implementing custom security solutions, often using externally developed software and hardware as well as taking a role of a system integrator.

Arguably the most renowned InfoSec firm in Korea is AhnLab, founded in 1995 and listed on the Korean tech stock exchange KOSDAQ. Unlike SK Shieldus, Ahnlab was not spun out of a large conglomerate but is instead a notable start-up success story. The company provides antivirus and online security software, network security appliances, firewalls, intrusion prevention systems (IPS) and unified threat management (UTM). The company has more than a 50% share of the Korean firewall and antivirus market in both the public and private sector. In line with the rise of cloud services and the demand from the market, AhnLab is also focusing on security consulting and developing cloud management solutions.

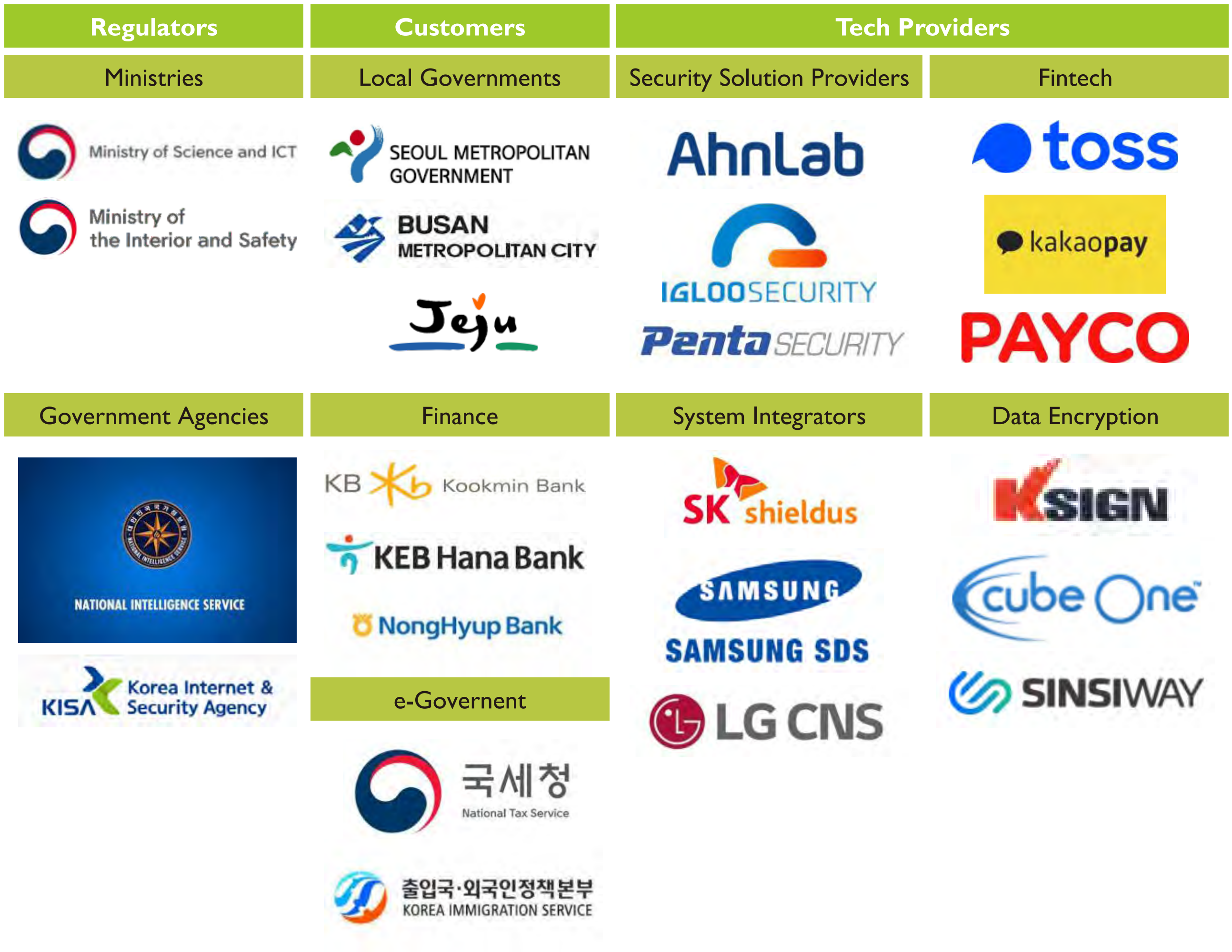
Other increasingly influential domestic players include WINS, a provider of network security, Igloo Security, an AI powered security information and event management provider, Penta Security Systems, a provider of data encryption technology, Initech, a security solution provider for the financial sector, as well as nProtect, the largest InfoSec company within the financial industry sector.

Table 4: Leading Market Players in Korea

Company	Website	Revenue	Employees	Key Products	Key Target Industries
SK Shieldus	www.skshieldus.com	£248m	6,496	Managed security services, consulting, SI, physical security	Enterprise
AhnLab	www.ahnlab.com	£110m	1,193	Antivirus software, online security, network security appliances, firewalls, IPS, UTM	Public Sector, Financial Institutions
SECUI	www.secui.com	£71m	403	Information protection solutions e.g., Intrusion prevention systems, anti-DDoS security systems, vulnerability analysis solutions, unified management systems	Electrical Equipment, Industrial
WINS	www.wins21.co.kr	£57m	476	Intrusion prevention, firewall, web application firewall, DDoS response, APT protection, integrated security monitoring, video privacy management systems, IoT	Enterprise
IGLOO SECURITY	www.igloosec.co.kr	£52m	924	Managed security service, enterprise security management	Business/Consumer Services
SGA Solutions	www.sgasol.kr	£25m	123	Antivirus solutions, server security solutions, firewalls, intrusion prevention systems, virtual private networks	Technology
Dream Security	www.dreamsecurity.com	£15m	198	Internet security solutions, electric devices, IT security services, wireless security, electric document security	Public Enterprise, Finance, Enterprise

Source: Intralink Research, multiple sources

Figure 3: InfoSec Ecosystem



04 OPPORTUNITY AREAS FOR BRITISH COMPANIES

Key Points

- Opportunities for British InfoSec companies exist particularly for applications in the areas of:
  - Internet banking and finance, public sector and national security, database encryption
- Personal identification technologies such as biometrics are of high interest to banks and fintech industry
- The government is investing large sums to protect public institutions against cyber espionage and other cyber threats, but public-sector bids can be challenging to compete in for foreign companies
- Strict privacy laws create opportunities for database protection and data encryption solution providers, particularly in healthcare, e-commerce and telecoms

INFORMATION SECURITY IN THE FINANCIAL INDUSTRY

Blockchain

Due to the focus on the Fourth Industrial Revolution and the rising interest from many Korean companies in cryptocurrencies, non-fungible tokens (NFT), and Central Bank Digital Currencies (CBDCs), investments in blockchain and virtual assets by major chaebol firms and banks have skyrocketed. The Bank of Korea is currently conducting a pilot project for issuing indigenous CBDC, anticipating that the demand will surge for 'custody' projects that allow digital assets to be securely saved in the virtual realm.

Table 5: Korean Banks and Blockchain

Banks	Revenue	Employees	Blockchain Plans
IBK	GBP 12.5bn	13,283	• Selected ReDWit, a provider of blockchain-based document management systems, as part of its start-up incubator program
Shinhan Bank	GBP 14.7bn	13,332	• Implemented an integrated authentication service using blockchain, called Decentralized ID (DID) • Won Ecosystem Transformation award at Enterprise Blockchain Awards for its contribution to the advancement of blockchain in the finance sector
Kookmin Bank	GBP 15.5bn	16,504	• Actively using blockchain technology for compliance, authentication, prevention of money laundering • Planning to issue digital assets on its platform 'KB Chain' to prepare for decentralized asset management
KEB Hana Bank	GBP 22.9bn	12,110	• Partnered with Kasa Korea, a blockchain start-up, to issue digital real estate beneficiary certificates and open user accounts
Woori Bank	GBP 17.1bn	13,825	• Tested Ripple's blockchain technology for overseas remittance in 2018 • Currently creating a JV with cryptocurrency start-up Coinplug for digital asset management

Source: Korea Institute of Science and Technology Information (KISTI) Market Report, 2021

The Korea Federation of Banks (KFB) and many Korean banks are also interested in the possibility of using blockchain to enable data sharing for connected banks without having to go through complex procedures. Shinhan Bank is preparing to utilize Stablecoin that will allow commission-free international transfers in less than a minute. Stablecoin has already been adopted by larger financial firms such as JP Morgan while Shinhan Bank is the first Korean bank to make the bold move. Stablecoin-based international transfer is known for its transparency and expandability.

The Korean fintech industry

The fintech start-up industry has grown rapidly in recent years to comprise approximately 600 fintech companies that are eager to exploit market opportunities neglected by the conservative traditional financial sector. The revenues of these local fintech companies grew by 13% over the past two years. Growth was observed across all sectors except cryptocurrency exchanges, which recorded a revenue dip of GBP 342m or 56.2%.

Closer Look

The financial industry in Korea is going through rapid transformation to adapt to the Digital Transformation and the Korean government's initiatives to create an economy based on the Fourth Industrial Revolution. In December 2021, 17 service providers including banks, financial institutions, card companies and fintechs launched the API-based "MyData" service followed by 36 another companies by summer 2022. The service is indended to allow consumers to access and manage their financial data more easily while guaranteeing their data privacy rights.

Although the key advantage to the "MyData" service is to ensure personal data security, personal information has already been leaked by Naver Financial and there have been glitches in the API information transfer by several banks. As the industry rushes to provide faster and more secure services, information security will be key for the FinTech industry to grow further.

Revenues of remittance and digital payment companies grew the most – revenues reached GBP 1.13bn (43% increase), followed by insurance information technology with GBP 106.4m (38.7% increase), foreign remittance with GBP 19m (278% increase), crowdfunding and P2P finance with GBP 15m (48.3%) and security and authentication with GBP 9.7m (7.5% increase). In addition, more than 50 dedicated fintech organisations have been established within traditional financial institutions, for instance Shinhan Bank's Shinhan Future's Lab or Hanwha Group's DreamPlus.

Table 6: Top 10 Fintech Start-ups by 2021

Company	Total Funding Received	Number of Employees	Solution
Toss	844.2m	2,198	Mobile financial service platform
People Fund	88.1m	1,703	Data-driven digital lender focused on consumer finance
Fount	33.4m	17,779	Solution asset management robo-advisor for passive investing
Naver Financial	676m	22,435	Financial service platform
LENDIT	21.7m	42,909	Platform connecting loan-investors with individuals seeking loans
True Balance	144.6m	819	Digital wallet solution
K Bank	87m	198,917	Online banking service
Rainist	63m	30,940	Credit card recommendation service based on spending patterns
Korbit	82.1m	746	Cryptocurrency exchange platform
Sentbe	8.4m	18,450	Fintech fund transfer service

Source: Intralink Research

A particularly active segment within the Korean fintech space is online and mobile payments. Making payments through an online payment solution has become a common trend in Korea. According to a National Assembly report on fintech, the amount of daily online payment transactions reached GBP 365m with an average daily volume of 18.2m transactions in the second half of 2021. Online payment services are provided not only by traditional banks, but also by IT companies like Naver and Kakao, electronics companies like Samsung Electronics and LG, as well as fintech payment services like Payco and PayPal.

There are also three online-only banks: Kakao Bank, K Bank and Toss Bank. Thanks to the online-only banks, biometric authentication technology using iris, voice, facial recognition, etc. has become the new standard service for improved ease of use and security, creating potential collaboration opportunities for domestic and foreign InfoSec companies.

Security measures initiated by fintech companies and now adopted by the traditional financial institutions, such as SMS approval, magnetic security transmission (MST) and near field communication (NFC) are commonly used as well. Many Korean banks are also showing increasing interest in blockchain and biometrics. With more fintech companies and traditional banks open to the idea of newer forms of security practices, this could be a potentially lucrative opportunity for UK companies to enter the Korean market.

The main areas of interest from Korean financial institutions in the coming years will likely include:

- biometrics
- data loss protection (DLP)
- transaction encryption and authentication
- digital payment protection
- blockchain

INFORMATION SECURITY FOR AUTONOMOUS VEHICLES

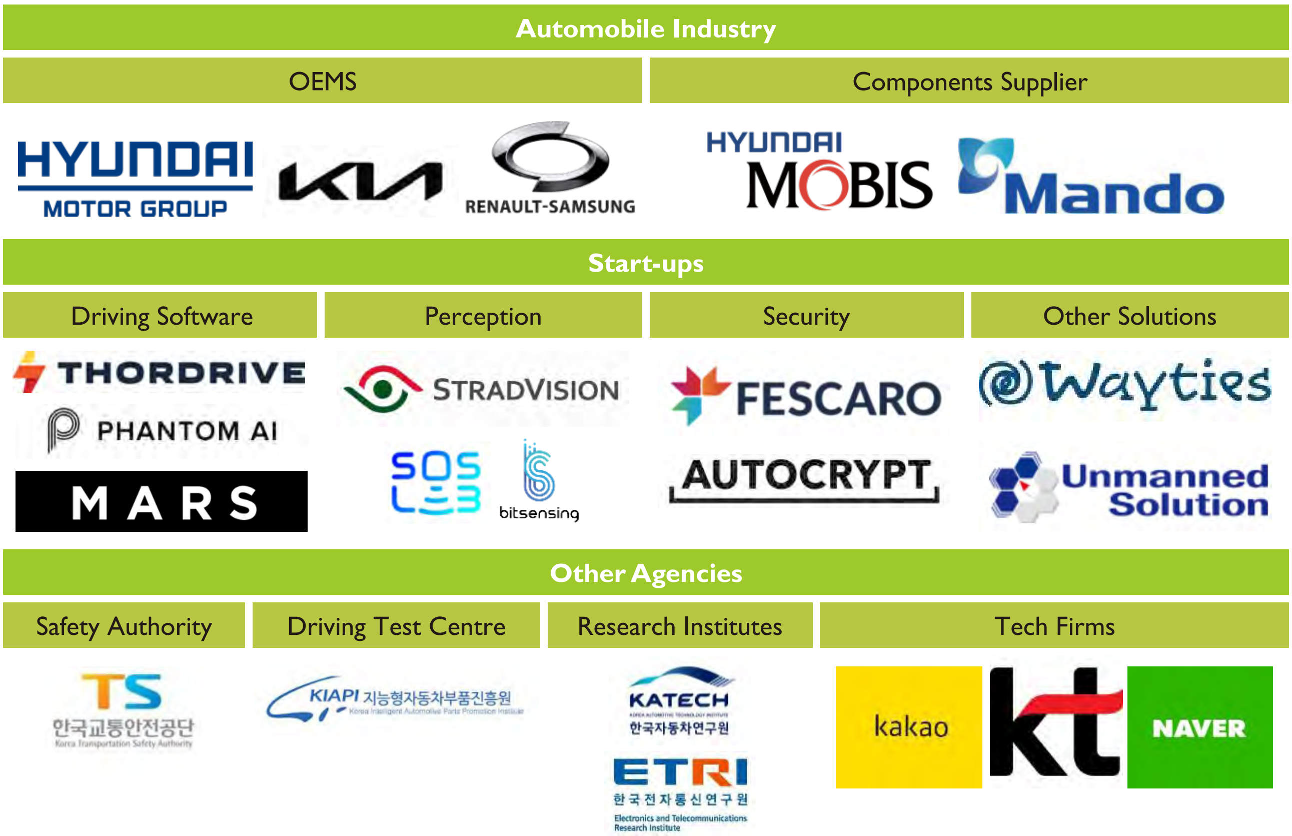
The range of possible connected products is growing, and one range of products that has received a great deal of attention is the automotive sector. According to IHS Markit's estimate, over 11.2m connected vehicles equipped with Vehicle-to-Everything (V2X) will be produced worldwide by 2024. Modern cars have numerous electronic control units and microprocessors, sensors, GPS, radio and cellular connectivity to the 5G network, all of which can be possibly hacked. With smart cars and connected cars seeming to be the future of the automotive market, many tier-one suppliers and automotive companies in Korea are focusing on the possibility of cyber-attacks on their vehicles.

In 2021, the Ministry of Land, Infrastructure and Transport (MOLIT) and MSIT has set out plans to create an infrastructure to construct Cooperative Intelligent Transport Systems (C-IST) based on dedicated short-range communications (DSRC) as a part of the Smart City initiative. As Hyundai Motors announced commercialisation of level 4 autonomous taxis by 2023, the government plans to construct Cooperative-V2X as well as 'WAVE' (a type of DSRC) along 2,400km of highway. A local security solution start-up, Ciot, will be providing the comprehensive security module and V2X security authentication module for the project.

Although the number of Korean start-up security companies is growing, only a few companies focus exclusively on car security. Examples of Korean companies active in the space include Fescaro, which develops and installs multiple cybersecurity software programs to protect key electronic control units, as well as AutoCrypt, a vehicle security solution spin-off from Penta Security, an established InfoSec player that is increasingly focusing on connected vehicle security applications.

Case Study: AutoCrypt	
Website	autocrypt.io
Problem	How to detect software security vunerabilities on connected vehicles
Solution	Develop a singular integrated 'Fuzzing' solution
Who implemented it?	Security Research Center within Penta Security and AutoCrypt
Overview	AutoCrypt, a company that spun off from Penta Security in 2019, focuses on developing products for V2X security. 'Fuzzing' tests are an integral part of detecting software vulnerabilities in connected and autonomous vehicles. AutoCrypt is the first company in Korea to develop integrated 'Fuzzing' solutions dedicated for the automotive industry. The technology allows vehicles to conduct the test autonomously through smart fuzzing technique, respond to various error codes without the presence of engineers and detect and analyse security vulnerabilities.

Figure 4: Major Korean Players in Autonomous Vehicle



INFORMATION SECURITY IN DIGITAL HEALTH

Digital Health is seen by many as a lucrative future market filled with possibilities. In addition, due to COVID-19, the need for remote medical services has surged. According to a survey conducted by the Korea Health Industry Development Institute (KHIDI), 76.9% of respondents replied that they wished to use their personal medical information to receive better treatment and manage their health.

To meet the demand, the Korean government is establishing a platform called 'My Healthway' by 2022 to collect bio-information of individuals as part of the Digital New Deal project. It will allow easy access to personal information across medical centres. However, network interconnectedness and handling sensitive personal data are increasing the need for InfoSec solutions as the world sees more ransomware attacks on hospitals. This sector also presents strong opportunities for UK companies, as the security of this data will be of the highest priority, and the medical market in Korea is an early adopter of the latest technologies from around the world.

Digital health is of high interest to many companies looking towards the future, and major Korean IT companies like Kakao and Naver have identified this as a growth sector. Kakao Group, the fourth largest corporation in Korea, has recently created a subsidiary company, Kakao Healthcare. By partnering with medical big data company Humanscape, Kakao plans to provide health monitoring services while incorporating blockchain technology to secure private user data.

The market for digital health InfoSec solutions will grow concurrently, with opportunities particularly in:

- authentication
- data encryption
- database protection
- medical IoT communication security

Closer Look

The pandemic has become a catalyst for growing interest in the area of digital healthcare. As the hyper-connectivity of modern societies creates vulnerabilities to hacking and ransomeware attacks, Korean digital healthcare firms are working towards receiving internationally recognized certifications such as 'ISO 27001' for information security and 'ISO 27701' for privacy security for digital healthcare products. Companies such as EOFlow, EDGC and Life Semantics have already acquired various ISO certificates and a growing number of Korean companies are looking to strengthen information security to meet the demands for data security in this rapidly growing industry.

INFORMATION SECURITY IN THE PUBLIC SECTOR

The typical public-sector customers of InfoSec technology companies include local governments e.g., the Seoul Metropolitan Government, Korea Immigration Service (KIS) or National Tax Service (NTS). The need to introduce adequate information protection is arguably more urgent in the public sector which has the citizens' privacy and safety at its core. There are three government agencies tasked with identifying, preventing and responding to cyber-attacks and state-level security threats: the National Cyber Security Centre (NCSC), KISA, and the National Police Agency's Cyber Terror Response Centre (CTRC).

Organized groups of hackers have previously targeted government agencies in Korea, compromising sensitive information and endangering the welfare of government officials and civilian employees alike. With regards to external hacking attempts, North Korea has always posed the largest threat. According to a former state-employed North Korean hacker, the country purportedly has 6,000 state-employed hackers specialising in cyber warfare and espionage. NIS has announced concerns for additional hostility from North Korea in 2022 due to the presidential election.

Although there have been growing concerns for securing networks and strengthening the information security of the public sector, according to research conducted by the NIS, out of 128 government organisations and public corporations, only 46% operated an InfoSec division. Further, 40% of these organisations had less than two employees dedicated to protecting their network. In addition, the cyber defence team of Korea Armed Forces is comprised of 1,000 soldiers, 50% of whom are still in training. It is feared and expected that Korea will suffer from a shortage of 10,000 InfoSec experts by 2025.

Industry Insider's Thoughts

We suspect that the Korean government uses its own standard at least partly to prevent foreign companies from entering the Korean market.

Sales engineer working for an international supplier of encryption services

Encryption solutions

The Korean government exhibits what might be perceived as protectionist tendencies when it comes to encryption solutions. NIS has so far approved two solutions: SHA256 and ARIA. For example, the global encryption standard is AES256, whereas the Korean public sector is required by law to purchase solutions with the SHA256 encryption model. This means that foreign companies wanting to enter the Korean market and supply to the public sector must adopt this encryption model. Moreover, ARIA is an open-source code, which few companies find acceptable. Very few foreign companies are using SHA256 or have registered with the government as approved suppliers.

Supplying information security systems to public institutions

Public institutions purchasing IT systems must procure systems that include security functions which conform to the requirements of the NIS. This generally means that they must be Common Criteria (CC)-certified. Products that include a password function for storing and communicating data such as section encryption and database encryption are required to include a verification cipher module. In 2021, the NIS expanded the number of products from 22 to 29 for the organization to certify constantly evolving IT products.

The security conformance verification system consists of a verification organisation and a testing organisation. NIS, the official verification authority, accepts applications for verification of security conformity and supervises the management of the test work. KISA provides detailed guidelines on and support for certification procedures.

With incessant cyber espionage threats and the relative weakness of Korean public institutions' cyber security systems, there is significant demand for government-grade information security solutions. The public sector recognises that the domestic InfoSec industry may not be able to satisfy all of its needs, so it is increasingly looking for overseas specialists in the field.

The key areas of interest include but are not limited to:

- encryption solutions
- anti-malware solutions
- DDoS and ransomware attack protection solutions
- cyber-threat detection solutions
- consulting services

However, due to the government's tight control over certification and solution selection processes, inexperienced overseas companies will find themselves disadvantaged against their domestic counterparts. It is advised that partnering with experienced domestic InfoSec technology distributors or system integrators is recommended as the primary route to market. The process of obtaining certification can take 6–12 months and because of the cost associated with obtaining additional Korea-specific certifications, a detailed cost-benefit analysis is strongly recommended.

Case Study: Korea Hydro & Nuclear Power (KHNP)	
Website	www.khnp.co.kr
Problem	How to ensure citizens' safety and protect vital institutions from cyber espionage
Solution	Create a public and private sector "cyber security control tower"
Who implemented it?	KHNP, KISA, National Intelligence Agency, private sector consultants etc.
Overview	In 2014, KHNP was hacked by North Korean hacker group, 'Kimsusy'. Nuclear reactor blueprints, sensitive technical specifications and personal information of over 10,000 employees were exposed. The hackers demanded USD 10 million in ransom to stop releasing the stolen data. The hackers were able to gain access to this data by performing coordinated phishing attacks on employees to intercept their passwords for months prior to the "meltdown". In response to this attack, the government announced measures to improve the physical and cyber security environment surrounding nuclear facilities which included requiring nuclear power plant operators to enhance their computer and information security systems. Due to the severity of the potential repercussions, multiple government agencies and private cyber security consultants got involved to create a nationwide "cyber security control tower" inside of the National Security Office (NSO) to develop strategies to combat cyber-attacks, foster technology adoption, and educate government workers on preventive measures. For this work, KHNP won second place in '2021 Cybersecurity Challenge' hosted by the NIS.

GENERAL ENCRYPTION SERVICES

Constant cyber-security threats combined with the need for conglomerates to ensure that their business secrets are not compromised indicates that the Korean data encryption platform market is growing quickly. The data encryption market has been maturing since 2017 and the market size reached GBP 291m in 2020, a 6% increase from the previous year. The demand is expected to rise as enterprises follow the data protection compliance. There is strong demand for solutions that can encrypt data within file systems and provide differentiated levels of access. In recent years, the Korea ON-Line E-Procurement Agency (www.g2b.go.kr) showed an 8% increase every year in encryption software purchasing plans.

Currently most data encryption providers in Korea are local companies including Penta Security Systems, KSign, eGlobalSystem (CubeOne) and SinsiWay. Both domestic and foreign solutions must receive Korea Cryptographic Module Validation Program (KCMVP) certification from the NIS to provide encryption solutions in Korea. As a part of adopting to Digital Transformation, Korean companies are increasingly pivoting to cloud services and the demand for secure server encryption is growing accordingly.

The demand for data encryption software exists in all market verticals that involve storage and management of user data. It is particularly high in areas such as:

- healthcare and medical services
- e-commerce
- telecommunications
- financial services
- marketing services

In order for foreign companies to serve the market well, it is recommended to apply a level of localisation for the solutions. For instance, appointing a local 24/7 customer support team along with a Korean-language version of the solution should be seen as necessary first steps.

05

MARKET ENTRY STRATEGIES

Key Points

- Direct sales into the large conglomerates is possible but on-the-ground support is strongly advised
- Using a sales team based outside of Korea is difficult due to language and cultural barriers and very high expectations for after-sales support
- Partnering with local systems integrators or value-added resellers is advisable for foreign companies
- Foreign companies can apply to participate in government-led projects but there are barriers:
  - Culture, language, business environment, etc.
  - Preference towards local businesses adding at least some value to the products or services

Korea offers many opportunities for UK businesses, with many large Korean corporations, financial and non-financial, actively developing fintech solutions or partnering with other companies for innovative services. The government's dedication to become a leader of the fourth industrial revolution and a rapidly developing local fintech market create a solid foundation for foreign businesses to test and introduce their fintech technology. However, UK businesses looking to engage in a strategic partnership or introduce their technology to Korea should consider both business-related and cultural factors. UK businesses can approach the Korean market through direct sales from the UK, by appointing a partner or by setting up an office in Korea.

Direct Sales from the UK

The simplest market entry option is for UK companies to sell or license a particular fintech technology directly to Korean end-users. The main downside of a direct sales approach is the lack of local language and time-zone support, as Korean companies tend to be particularly demanding of their partners. This can be mitigated by using a local agent or business development consultancy, such as Intralink, capable of bridging time-zone, language and cultural gaps without the long-term commitment of local incorporation and hiring. Market-specific factors to consider include:

- Do we have a strong differentiator – something that sets us apart from our competitors in the market?
- Do we have a strong track record in other major markets? Korean companies are not easily convinced to use a new, disruptive technology as a first-mover without case studies
- Are we willing to localise the product for the market and/or for local regulations, if necessary?
- Are we ready to provide a Proof of Concept (PoC) at little or no cost to the customer? Korean companies will look to drive the price down and will not commit before proving the value through testing
- How do we provide after-sales support? Korean customers expect high-quality, local-language support

Appointing a Reseller or Distributor

A more common way to approach the market is to seek a partnership with an established local company which complements your product, has experience in the target sector and can help navigate the legal environment. A local channel partner, perhaps a systems integrator (SI), can provide services such as pre-sales, sales, consulting, installation, technical training, service maintenance, technical support and system integration in the Korean market. Even large multinationals take this route in the early stages of market entry. Market specific factors to consider when seeking a partner include:

- Does the partner already serve the type of customer that we do?
- Does the partner have a good understanding of the market in general and my particular application?
- Does the partner already offer solutions similar or complementary to our offering?
- Is the partner focused on short-term wins or will they be able to drive our business in the long run?
- Does the partner have specific experience

with public sector projects?
- Are we comfortable communicating with the local partner and are they transparent with us?

Establishing a Local Presence

There are broadly three ways of establishing a local presence: (1) a liaison office, (2) a branch office or (3) a local corporation through foreign direct investment (FDI). Setting up a liaison office is a simple process; but a liaison office can only perform non-profit generating activities in Korea such as market surveys, research and development and quality assurance. Setting up a branch office can be a complicated process that requires documentation to be translated, but it allows for sales activities and the exchange of revenues with the head office. The most common process for an overseas company to open a branch office in Korea is through FDI, where an initial investment exceeding approximately GBP 68,000 is made by the head office, which in return owns stock in the branch. The local corporation leads independent activities and is authorised to perform direct transactions. Market-specific factors to consider when establishing a local presence in Korea include:

- Is our business generating enough revenue in Korea to consider a local presence? Businesses usually consider establishing a local presence after several years of sales (either direct or through a partner)
- Is Korea a strategic market for us, either in terms of securing use-cases or securing further funding?
- Do we need to engage in profit generating activities?
- Will we transfer staff from our head office or hire local staff? In Korea, visas can be difficult to secure for foreign employees and social insurance contributions and severance pay must be paid to all staff that complete one year of employment. An employer’s share of these costs equates to 18% of salary
- What location shall we pick for our local presence? Scouting, negotiating, and conclusion of contracts are time-intensive processes that often are hard to conclude without local support

For further information please contact:

Soyeon Kim
Project Manager
soyeon.kim@intralinkgroup.com

Jonathan Cleave
Managing Director
jonathan.cleave@intralinkgroup.com

MADE IN THE UK
SOLD TO THE WORLD

Department for
International Trade

The Department for International Trade (DIT) helps businesses export, drives inward and outward investment, negotiates market access and trade deals, and champions free trade.

Legal disclaimer

Whereas every effort has been made to ensure that the information in this document is accurate the Department for International Trade does not accept liability for any errors, omissions or misleading statements, and no warranty is given or responsibility accepted as to the standing of any individual, firm, company or other organisation mentioned.

CONTENT PARTNER

Intralink

Intralink is an international business development and innovation consultancy specialising in East Asia. The firm's mission is to make commercial success in new global markets fast, easy, and cost effective.

Published May 2022
by Department for international Trade