Information Security South Korea

Market Intelligence Report

Department for International Trade
Report prepared by Intralink Limited

July 2018

TECHNOLOGY IS GREAT
BRITAIN & NORTHERN IRELAND

About Intralink

Intralink is an international business development consultancy with a deep specialism in East Asia.

Our mission is to make companies' growth in overseas markets fast, easy and cost effective.

We have 80 multilingual employees, a 28-year track record and offices in London, Silicon Valley, Boston, Shanghai, Tokyo, Seoul and Taipei. We enable Western companies to expand in Asia, and Asian companies to expand in the West.

We do this by providing the in-country expertise to identify a company's market opportunity, secure sales and drive its business growth. Our teams are immersed in the business practices, cultures and customs of their local markets.

And we are different from other consultancies as we do not just develop market expansion strategies for our clients – we play a hands-on role in building their businesses.

Through our Surrogate Sales Program™, we close deals, generate revenues and, when a client is ready, help them set up a permanent in-country presence through a local subsidiary, partnership or acquisition.

We also offer a range of additional services including market opportunity assessments, distributor and supplier searches, investment co-ordination and local representation.

Our clients are companies from start-ups to multinationals in the automotive, energy, healthcare, electronics, telecoms and other high-growth sectors. We also work with governments and economic development agencies to promote exports and attract foreign direct investment.

Intralink

Table of Contents

Table of Figures

Table of Tables

1. Introduction

South Korea (Korea) is one of the most connected nations on earth and the ICT infrastructure that supports this connectivity has proven vulnerable to cyber-attacks. As the country races towards the so-called Fourth Industrial Revolution, the amount of data being produced, stored and transmitted is increasing at a phenomenal rate. In parallel, Korea is facing a proliferation of cyber threats, domestically and internationally, with many recent attacks believed to have originated from China and North Korea. Ensuring the security of personal, corporate and government data, therefore, is recognised as essential not only for the health of the Korean economy but also for the security of the state itself, and demand is strong for information security (InfoSec) solutions that can help in this effort.

The size of the Korean InfoSec market was reported to be GBP 1.8 billion in 2017 – an increase of 10.3% over 2016 – and, according to a recent report prepared by the Korean National Assembly, the number of cyber-attacks and malicious codes aimed at Korea increased dramatically from 78,000 in 2013 to 3.4 million for the period between January and August of 2017 alone. Nevertheless, Korea is still heavily reliant on overseas solutions to meet its cyber security needs. Imports of InfoSec solutions stood at GBP 619 million in 2017, clearly demonstrating the demand for solutions from overseas InfoSec solution providers.

The market is dominated by multinationals like Microsoft and Symantec, which usually work with large corporate clients, and exclusively-local solution providers, such as SK InfoSec and AhnLab, which tend to work with smaller companies and the Korean government. There are also value-added resellers (VARs), systems integrators (SIs) and security consultancies which partner with local and overseas solution providers. The market is characterised by outdated protocols and a regulatory framework that is often at odds with global best practices. Indeed, dated regulations and infrastructure are often cited as reasons why local InfoSec companies are not globally competitive and why large customers prefer to work with overseas suppliers.

For UK InfoSec companies, the lack of global best practices, relatively weak domestic InfoSec companies and increasing deregulation in the area all combine to make Korea a potentially attractive market. Opportunities in the market include finance (e.g. internet banking, digital payments, biometric identification, fraud detection, blockchain), solutions for convergence industries such as autonomous vehicles and digital health, cyber-terrorism prevention, DDoS and other cyber-threat detection, InfoSec consulting, as well as general data encryption and encryption software for e-commerce.

The Korean InfoSec market presents challenges but also potential rewards for overseas companies in the industry. Although domestic capabilities are improving and there is a growing pool of local InfoSec start-ups that could rise to pre-eminence in the near future, there are clear opportunities in the near term for British companies with the right solution and go-to-market strategy.

2. Korea - An Overview

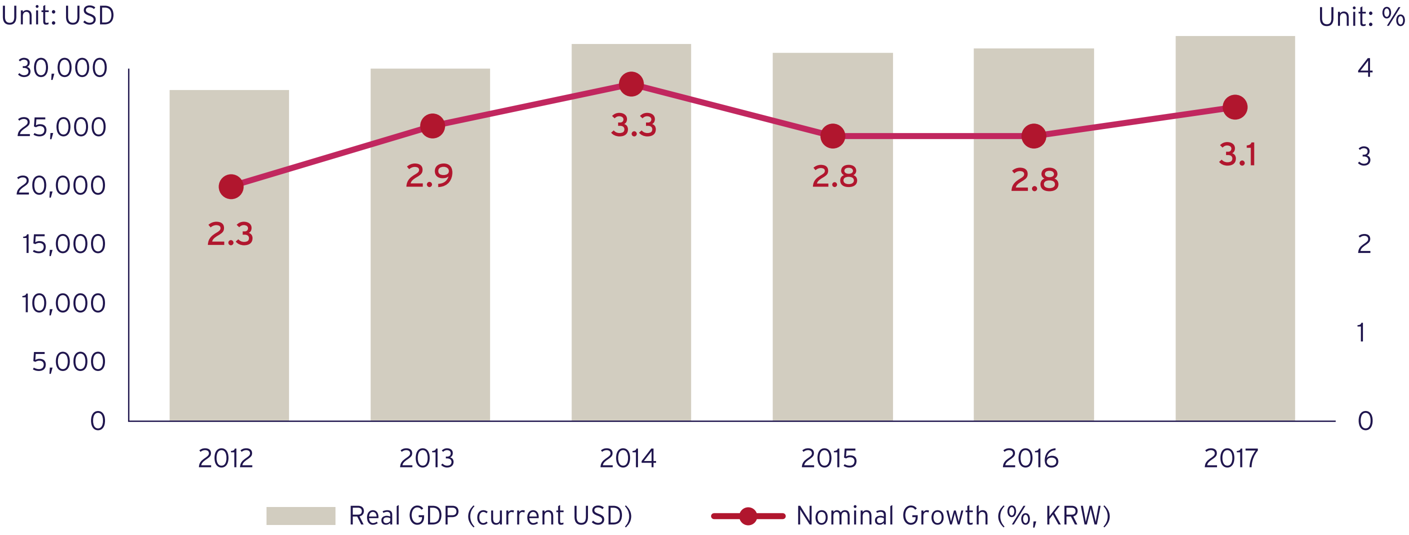
KEY POINTS

- Korea has climbed out of poverty to become a technology powerhouse over the last 60 years
- The country is the world's 11th largest economy with a GDP of just over GBP 1 trillion
- tIt has maintained annual GDP growth of around 3% in recent years

In the space of just 60 years, Korea has developed 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 areas of electronics and information communications. As well as dominating the global semiconductor industry, Korea has leap-frogged its peers in terms of ICT infrastructure (smartphone penetration rate, broadband speed etc.) and this, coupled with a demanding and technology-embracing population, means Korea is becoming an economy driven by creativity and innovation.

With a population of 51 million, Korea boasts the 11th largest economy, a GDP of GBP 1.11 trillion in 2017 and a per capita GDP of GBP 22,218 in the same year. Whilst not experiencing the growth witnessed in China, the country has maintained strong annual growth for a developed economy of around 3% in recent years, outpacing its regional rival, Japan. Korea's trade dependency ratio is extremely high at over 80% and its economic performance is heavily affected by the economies of China, the US and Japan. Trade and investment flows between Korea and the EU are growing as a result of the FTA that came into effect in 2011. Trade between Korea and the UK specifically has grown rapidly over that period and both countries have expressed a strong desire to conclude a trade deal once the UK leaves the EU.

Figure 1: Korean GDP per Capita (2012 - 2017)



Source: World Bank

3. The Information Security Market in Korea

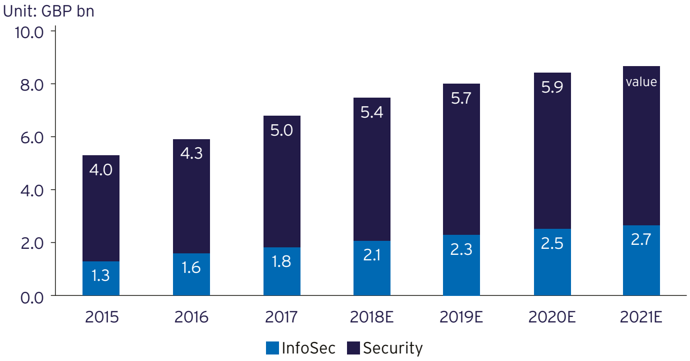
KEY POINTS

- The Korean InfoSec market stood at GBP 1.8 billion in 2017; an increase of 10.3% over 2016
- The number of attacks originating from North Korea and China has been increasing in recent years
- Korea is a net importer of InfoSec solutions, importing 10 times more than it exports
- In 2015, the Korean government laid out the "K-ICT Security Development Strategy and the Act on the Promotion of Information Security Industry" in an effort to strengthen its domestic competitiveness
- Key domestic players include SK InfoSec, Ahnlab, Hancom Secure, WINS and IGLOO SECURITY

Korea takes pride in being one of the world's most connected nations and is actively working to build its competency in sectors such as the Internet of Things (IoT), data analytics and artificial intelligence (AI). The rise of these sectors is leading to greater connectivity and a burgeoning data economy, which in turn requires enhanced information security. Valued at GBP 1.8 billion in 2017 with a 10.3% annual growth rate, the InfoSec market is one of the most dynamic sectors within the larger Korean IT market.

According to a survey conducted by the Korea Internet and Security Agency (KISA), in 2017 there were over 332 information security enterprises in Korea, holding over 2,000 patents related to cyber security. The share of InfoSec in the overall GBP 6.8 billion security market is growing, rising from 24% in 2015 to 26% in 2017, and is expected to account for 31% by 2021.

Figure 2: Sales for InfoSec and Physical Security Sector



Source: Survey for Information Security Industry in Korea: Year 2017 and Byline Network

Nevertheless, Korea is still heavily reliant on overseas solutions to meet its cyber security needs. Imports of information security solutions, which stood at GBP 619 million in 2017, were almost 10 times greater than exports clearly demonstrating the strong demand for solutions from overseas InfoSec providers.

3.1 Cyber Threats in Korea

With ever-expanding device connectivity comes an increasing need for security measures to protect data. According to a recent report prepared by the Korean National Assembly, the number of cyber-attacks and malicious codes aimed at Korea increased dramatically from 78,000 in 2013 to 3.4 million for January to August 2017 alone.

Due in part to its vulnerable geopolitical situation, Korea has experienced an increasing number of attacks alleged to originate from North Korea and China, making information security a key priority of state. In March 2013, major broadcasters such as KBS, MBC and YTN, and financial institutions such as Shinhan Bank and Nonghyup, suffered computer network failures. Upon investigation, the attacks were judged to have originated from North Korea. Similar signatures were also found in an attack on the Korea Hydro & Nuclear Power Company. Most recently, hackers based in North Korea succeeded in stealing GBP 4.9 million worth of cryptocurrency.

Next to these external risks, Korea is experiencing security threats originating domestically. According to the security company Imperva, in 2016, Korea had the largest number of DDoS attacks originating in any one country –three times more than experienced by Russia, which was ranked second. In fact, Korea’s DDoS responsibility was greater than the next three countries combined.

Although cyber security is recognized by the government as a matter of national security, Korean companies still trail in InfoSec competency compared with companies in 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. According to a 2017 survey by the Ministry of Science and ICT, 48% of companies interviewed stated that they plan purchase information security products or services – a 15.6% increase from the previous year. The rising threat, increased threat perception and lack of domestic capabilities all combine to present strong opportunities for British InfoSec solution providers.

Closer Look

In 2014, 27 million Korean ID numbers were stolen by hackers who exploited lax security of several large Korean online gaming, gambling and entertainment sites. The police reported this was a co-ordinated effort between over a dozen South Korean and Chinese hackers, all of whom were caught but not before they had sold the information on the black market. The group used the personal information to steal and resell online game currencies and other virtual assets.

Two factors were identified as enabling such an extensive attack:

1. Loose security measures on the targeted websites

2. Weak inherent security of the ID number system in Korea (the 13-digit number is not randomised and includes a person's date of birth and gender information), which allowed the hackers to further exploit the personal identity information they obtained

3.2 Korea's Information Security Policy

The Korean government has been actively working towards increasing the competitiveness of domestic firms in the InfoSec industry. This policy was reflected in the 2015 "K-ICT Security Development Strategy and Act on the Promotion of Information Security Industry," in which the previous government rolled out plans to invest heavily to spur the growth of the sector.

President Moon Jae-in, who came to power in May 2017, reaffirmed the policy priority announced under the previous Park Geun-hye administration to focus on the so-called Fourth Industrial Revolution which will necessarily require an emphasis on sub-sectors with strong InfoSec requirements such as fintech and IoT security. Towards this end, the Moon administration has formed a special 25-person committee made up of experts from both the private and public sector to provide concrete implementation suggestions.

The Korean government has identified blockchain technology as a particular focus and will invest approximately GBP 10 million in blockchain R&D and trial services to foster the emergence of a blockchain ecosystem. Another element of this initiative is the enactment of facilitating legislation, albeit with a focus on non-cryptocurrency applications (see section 4.1.2). Apart from blockchain, the government also identifies intelligent CCTV, encryption and biometric authentication as points of focus.

3.3 The Regulatory Environment

The Korean information security industry began to emerge in the mid-90s and the Korea Information Security Industry Association (KISIA) was formed in 1998. In 2001, The Korean government introduced a certification system called "Information Security Management System" (ISMS). The ISMS is a comprehensive system for establishing, managing and operating organisations' IT infrastructure to protect key information assets against outside threats. Since its introduction, most public institutions have been required to use security solutions that are ISMS-certified. The requirement also extends to IT infrastructure companies such as internet service providers and data centres, as well as information service providers of a certain size (more than around GBP 700,000 in sales in the previous year or more than 1 million average users a day for three months).

Korea has established itself as one of the toughest jurisdictions for personal information protection and privacy compliance in the world. The Personal Information Protection Act (PIPA), which was enacted in 2011, contains eight Personal Information Protection Principles. They require personal information to be collected for specific and lawful purposes and not used for further unauthorised purposes. The principles require personal information managers to ensure all information is accurate and held securely, to disclose their privacy policy and to anonymise information wherever possible. It contains separate rules for the initial collection and use of personal information and for any subsequent different uses or transfers to third parties. PIPA also has specific rules applicable to business transfers and other corporate transactions.

Many local as well as foreign companies in the data and e-commerce industries find personal information protection and privacy regulation in Korea to be amongst the most challenging aspects of doing business. The regulations are comprehensive and complicated, while still managing to be vague where it matters – mainly in distinguishing between what data is personal and identifiable and thus out of reach for commercial purposes, and what data is sufficiently anonymous that its use is permitted for analysis. For instance, under PIPA, not only individuals' names and birthdays are protected, but also images and voice recordings.

The legislation is also backed by extensive enforcement mechanisms, including provision for data subject class action suits. Korea instituted Asia's first "revenue-based penalty" under its IT Network Act whereby companies in breach of privacy regulations can be penalised by up to 3% of their annual revenue.

“

Industry Insider's Thoughts

If there is a government drive, things can move very quickly. Recent improvements in fintech, flexible certification approvals and other liberal movements in this field show that change is really happening in Korea.

Head of Big Data Centre – BC Card

3.4 Leading Domestic Players

Korea has several large players in the information security industry which supply primarily to the local market. The largest information security company in Korea is SK InfoSec – an affiliate of the SK Group and sister company of SK Telecom, Korea's largest mobile operator. The company specialises in enterprise-grade security solutions including server protection, security platforms etc. SK InfoSec also offers security consulting and designs and implements custom security solutions, often using externally-developed software and hardware, while acting as a systems integrator (SI).

Another large player is S1, a Samsung Group affiliate. With revenue in 2017 of around GBP 1.3 billion, S1 has by far the largest revenue among InfoSec-related companies. However, the company's main business line is CCTV and other surveillance technology, with InfoSec representing a smaller business segment for which S1 does not publish separate financial figures. Within InfoSec, S1 supplies anti-virus programs as well as security control services, which include security equipment rental, VPN operation and anti-intrusion monitoring.

Arguably the most renowned InfoSec firm in Korea is Ahnlab, founded in 1995 and listed on the Korean tech stock exchange KOSDAQ. Unlike SK InfoSec, Ahnlab was not spun out of a large conglomerate but is instead a 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 almost a 50% share of the Korean firewall and antivirus market.

Other increasingly influential domestic players include Penta Security Systems, a provider of data encryption technology, Fasoo.Com, Inc., which offers a range of security products including file-based security solutions, as well as nProtect, the largest InfoSec company within the financial industry sector.

Closer Look

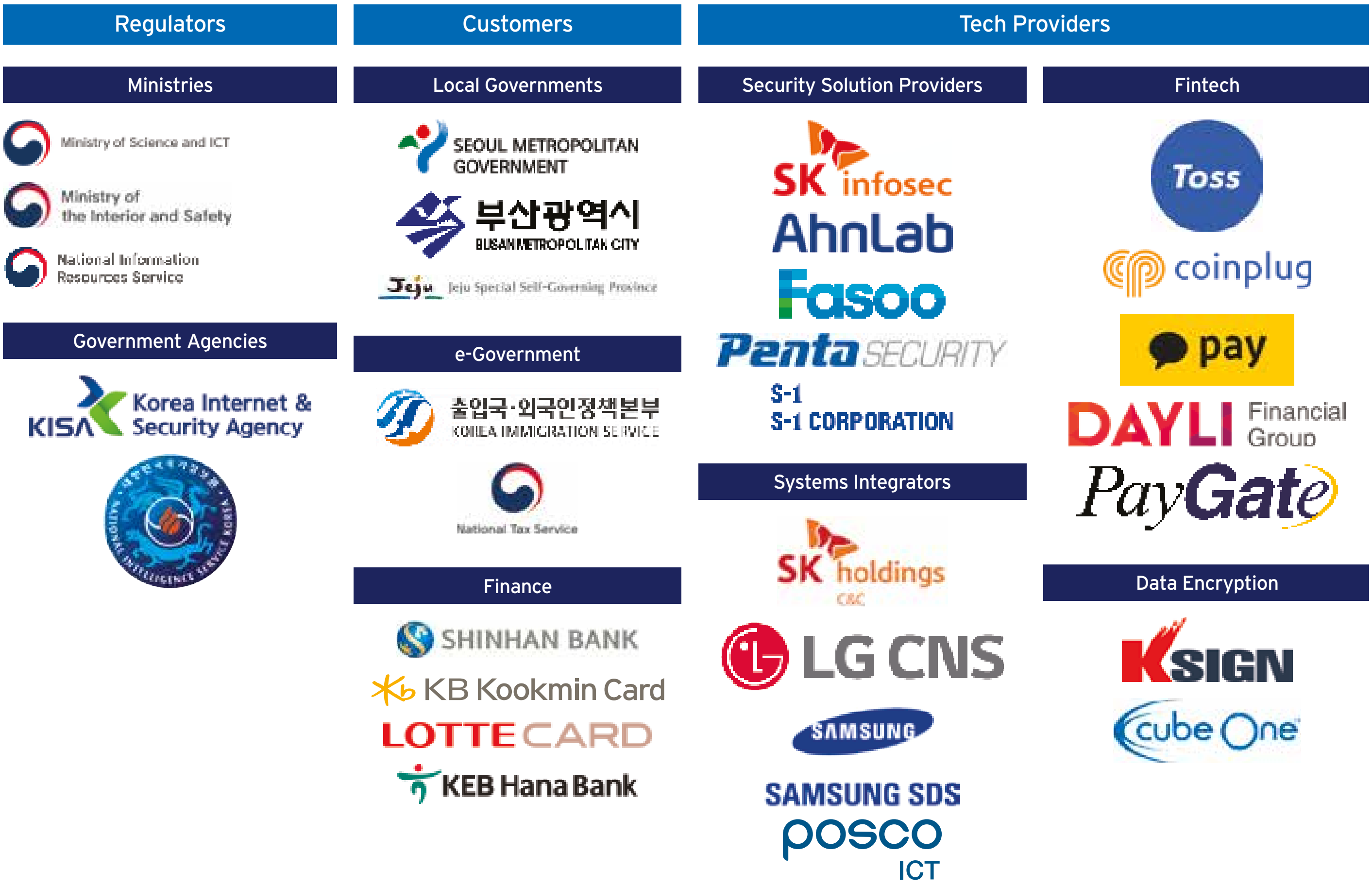
Korea Telecom (KT), Korea's largest broadband internet and second largest MNO, is highly regarded globally in terms of cyber security. KT Cyber Security Center, in Gwacheon City, is a state-of-the-art network security and internet traffic monitoring centre. A team of 50 InfoSec specialists uses secure server protection solutions adopted from global providers. The organisation also develops its own in-house software including malicious packet detection and protection. KT is believed to be the safest network in Korea and among the top five in the world. A source from the Cyber Security Center said that, while KT currently works with external vendors on "water-tightening" its own network, it may start selling its carrier-grade security software in the near future.

Table 1: Leading Market Players in Korea

Company	Revenue	Employees	Key Products	Key Target Industries
S1	1.28bn	6,150	CCTV and security hardware, VPN, antivirus, anti-intrusion monitoring	Enterprise
Ahnlab	110m	900+	Antivirus, Online Security, Network Security, Firewalls, IPS and UTM	Public Sector, Financial Institutions
SK InfoSec	108m	1,065	Managing Security Services, Consulting, SI	Public Sector
SECUI	52.4m	272	Intrusion prevention systems, anti-DDoS security, vulnerability analysis, unified management systems	Financial Institutions, Gaming
WINS	48.9m	392	Intrusion prevention, firewall, DDoS response, APT protection, integrated security monitoring, video privacy	Public Sector, Financial Institutions
IGLOO SECURITY	39m	718	Managed security service and enterprise security management	Enterprise
KICA	22m	73	Licensed Korean certification authority; provides identity confirmation, secure transaction guarantees, compensation system	Public Sector, Financial Institutions
SGA Solutions	18.9m	147	Antivirus, server security, firewalls, intrusion prevention and VPN	Public Sector
Fasoo	15m	289	Secure printing solutions	Financial Institutions, Gaming
Penta Security Systems	15m	200	Firewalls, encryption, and authentication	Public Sector, Financial Institutions
NICSTECH	13.7m	116	Personal/enterprise network security, web/mobile service implementation	Enterprise
Genians	13.6m	106	Cloud-managed network access control, IT security services	Public Sector, Financial Institutions
Hancom Secure	13.4m	122	Online integrated security solutions	Public Sector
Raonsecure	11m	143	Security solutions development and consulting	Financial Institutions, Gaming
Inca, nProtect	8m	200	Antivirus software, online security	Public Sector, Financial Institutions

Source: Intralink Korea

Figure 3: InfoSec Ecosystem



Regulators

Ministries

Government Agencies

Customers

Local Governments

e-Government

Finance

Tech Providers

Security Solution Providers

Systems Integrators

Fintech

Data Encryption

Ministry of Science and ICT
Ministry of the Interior and Safety
National Information Resources Service
KISA Korea Internet & Security Agency
NATIONAL INTELLIGENCE SERVICE KOREA
SEOUL METROPOLITAN GOVERNMENT
부산광역시 BUSAN METROPOLITAN CITY
Jeju Jeju Special Self-Governing Province
출입국·외국인정책본부 KOREA IMMIGRATION SERVICE
National Tax Service
SHINHAN BANK
KB Kookmin Card
LOTTE CARD
KEB Hana Bank
SK infosec
AhnLab
Fasoo
Penta SECURITY
S-1 S-1 CORPORATION
SK holdings C&C
LG CNS
SAMSUNG
SAMSUNG SDS
posco ICT
Toss
coinplug
pay
DAYLI Financial Group
PayGate
KSIGN
cube One

4. Opportunity Areas for British Companies

KEY POINTS

- Opportunities for British InfoSec companies exist, particularly for applications in the following areas:
  - Finance (internet banking, digital payments, biometric identification, fraud detection, blockchain)
  - Solutions for new convergence industries such as autonomous vehicles and digital health
  - Public sector applications and critical industry applications as well as related consulting services
  - Cyber terrorism prevention, encryption, DDoS and other cyber-threat detection
- Microsoft ActiveX-based security solutions, once a standard, are now being phased out, creating opportunities for new technologies to be applied in areas such as e-commerce
- The government is investing large sums to protect public institutions against cyber espionage and other cyber threats, but public-sector bids can be challenging for foreign companies

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 and marketing services and new convergence industries such as the autonomous vehicle market. Public institutions have a clear need for such solutions, although these opportunities may be more difficult for a British company to benefit from, especially without a partner in the form of a local value-added reseller or systems integrator.

“

Industry Insider’s Thoughts

The UK is strong in fintech and financial security. Traditionally a manufacturing country, Korea needs more service sector technology, particularly in blockchain, AI and fintech.

President of the Korea Association of Chief Information Security Officers

4.1 Information Security in the Financial Industry

4.1.1 Browser Security Solutions

The Korean banking and finance industry has been relying on ActiveX since the late 90s. While the protocol has largely fallen out of use globally, ActiveX remains in wide use in Korea, particularly in online banking and e-commerce. There are three reasons Korea has continued to use this obsolete technology: 1) banks and payment services have been obliged by law to live up to certain security standards, 2) the country’s IT security infrastructure has been built on the ActiveX platform and it is “locked in”, and 3) domestic security companies are reluctant to abandon a lucrative source of revenue.

“

Industry Insider’s Thoughts

ActiveX is a software framework that was cutting edge in 1996 and became Korea’s lasting weapon of choice. But it has devolved into a technology whose security is so flawed that Microsoft’s proudest achievement in its new Edge browser was its removal. It is ridiculous that banks are still using it.

Beyond Security - CEO

The root of Korea's reliance on this antiquated software goes back to 1999 and the enactment of the Digital Signature Act, which required a digital certificate issued by a financial institution to be installed on any computer used for online financial transactions, including purchases. In response, the Korea Internet Security Agency (KISA) developed a 128-bit block cipher called SEED and selected ActiveX control to run it on Internet Explorer, the dominant browser. Continued development has focused almost exclusively on Microsoft's ActiveX technology, with all web applications for e-government, banking, and online shopping being built on ActiveX. Moreover, government and financial institutions chose to place the increased burden of conforming to security protocols on the end user, i.e. requiring users to download ever-more security programs. By contrast, European financial institutions built security protocols into the back end, displaying friendly and functional UIs to the end user.

The Korean government has identified continued reliance on ActiveX as an impediment to the development of the Korean e-commerce and fintech industries and put forward a plan to start by removing as much as 90% of ActiveX from the country's 100 most popular websites, including eliminating plug-in policies from all government websites by 2020. It is also extending financial support to small and mid-sized firms to adopt web standards which use solutions which can replace ActiveX.

As local reliance on ActiveX has resulted in many local Korean IT security companies and web developers failing to keep abreast of other emerging security standards, the phasing out of ActiveX represents an opportunity for UK companies offering modern authentication and encryption solutions, such as solutions based on HTML5.

4.1.2 Blockchain

The focus on the so-called Fourth Industrial Revolution and the sudden interest by a great number of Koreans in cryptocurrency like Bitcoin, Ethereum and Ripple has made terms that were only familiar to specialists recognisable to most Koreans. According to Coinjournal, Korea's bitcoin market share was 8.7% in 2017 and its blockchain market is estimated to reach over GBP 233 million by 2020. Many sectors including banking and finance consider the possibility of using blockchain technology a promising area to strengthen both ease of access and information security.

Until the start of 2017, cryptocurrency went largely unregulated but, due to the alarming rise in cryptocurrency speculation, Korea's financial regulators decided stringent regulations were required and announced measures to curb speculation and illegal activity. These measures include the banning of ICOs in September 2017, the restriction of all foreigners, including residents, non-residents and ethnic Koreans with foreign citizenships, from trading cryptocurrencies in Korea, real name verification requirements and a ban on virtual bank account usage for cryptocurrency trading.

Following the enactment of these restrictive measures, Kang Young-soo, head of the Korean Financial Services Commission's (FSC) cryptocurrency division, announced that the FSC was exploring plans to advance blockchain-related technologies and would try to regulate crypto-trading showing that, while cautious about cryptocurrency trading, the Korean government is supportive of blockchain as a fintech and information security technology to facilitate other public and private sector applications.

Enthusiasm for non-cryptocurrency applications of blockchain is also reflected in private sector initiatives. Both established firms and start-ups have seen the potential of blockchain. For example, Samsung SDS launched its own blockchain platform, Nexledger, in July 2016. Samsung affiliates have used this solution for authenticating digital documents at credit card firm Samsung Card and signing digital contracts at battery maker Samsung SDI.

The Korea Federation of Banks and its members are also interested in the possibility of using blockchain to allow connected banks to share data without having to go through complex procedures. IBK, Shinhan bank, Kookmin bank, KEB Hana bank and Woori bank have signed up to R3's Corda, the open-source distributed ledger platform. These companies are planning to develop their own blockchain platform.

Table 2: Korean Banks' Plans for Blockchain

Banks	Revenue (GBP)	Employees	Blockchain Plans
IBK	9.1bn	12,183	Mutually co-operating with fintech company Korbit Created a department and workshop for Blockchain Started a fintech and blockchain hackathon with KISA
Shinhan Bank	10.4bn	13,333	Has started the development of an integrated authentication service using blockchain technology Looking for a blockchain model that allows for remittance of foreign currency
Kookmin Bank	11.7bn	17,548	Working on a security system that does not require real name verification since 2016 Co-operating with fintech company Coinplug on a blockchain verification security and prevention system Planning to integrate FIDO's biometric technology for transactions
KEB Hana Bank	18bn	7,570	First company in Korea to join the R3 consortium Planning on integrating FIDO's biometric technology
Woori Bank	13.7bn	13,647	Developing blockchain in the financial sector with eight departments and four affiliated companies

Source: KISTI Market Report, 2017

Table 3: Leading Players in the Korean Blockchain Market

Banks	Revenue (GBP)	Employees	Sector	Blockchain Development
Samsung SDS	3bn	12,963	Information technology	Launched blockchain platform, Nexledger, with start-up company Blocko
SK C&C	1.9bn	194	IT consulting, outsourcing, system integration, and system maintenance and repair	Developed a logistics system based on blockchain technology
LG CNS	1.3bn	5,425	IT Consulting, system integration, and outsourcing services	Partnered with Woori Bank to integrate AI into a blockchain platform
Kakao/ Dunamu	562m	2,490	Communication, media, content, games, lifestyle, fintech, and search engine	Will invest in 65.3m in local cryptocurrency exchange Upbit
Coinplug	5.4m	39	Cryptocurrency exchange platforms, exchange marketplace, electronic wallet service, and online point-of-sales service platforms	Working with various Korean banks on authentication infrastructure and converting card reward points to bitcoins
Streami	1.3m	40	Develops and offers blockchain based solutions for connecting and streamlining of financial networks	Operates cryptocurrency exchange GOPAX

Source: KISTI Market Report, 2017

4.1.3 Korea's Fintech Industry

The fintech industry has grown rapidly recently with Yonhap news reporting investments related to fintech business jumping to GBP 507 million in June of 2017 from 309 million in 2014, making it one of the fastest growing sectors in the local start-up scene. The previous Korean government announced in 2016 that it would contribute GBP 1.9 billion over the next three years to develop the Korean fintech industry. In addition, more than 50 dedicated fintech organisations have been established within traditional financial institutions such as Shinhan Bank's "Global Fintech Lab" and Hanwha Group's "Future Strategy/Fintech Division".

A particularly active segment within the Korean fintech space is online and mobile payments. According to a national assembly report on fintech, the amount of online payment transactions jumped from GBP 8.8 million a day with an average daily volume of 44,200 transactions in 2016, to almost GBP 32 million with 1.4 million transactions by February 2017. Online payment services are provided not only by traditional banks but also by internet companies like Naver and Kakao, electronics companies like Samsung Electronics and LG, as well as fintech payment services like Payco and PayPal.

Related to payments, further market innovations can be seen within the transaction authentication market. Previously, users had to enter their card number during each transaction, and for amounts above 300,000 won (approx GBP 200), an ActiveX certificate was required. By contrast, fintech services allow users to complete transactions with only a password. In such transactions, the financial institution automatically performs additional authentication based on Automatic Response Systems (ARS) which does not require software to be installed. Additional security measures recently embraced by financial institutions, include SMS approval, magnetic security transmission (MST) and near field communication (NFC).

The Korean financial services landscape has undergone further changes through an initiative to increase competition and innovation in the banking sector by allowing the creation of online banks. In September 2015, the Bank Act was amended to remove the requirement that a bank should have a physical presence. In November 2015, K-bank, the first internet bank with no brick-and-mortar branches, was granted a licence. This represents a major disruption to Korean banking and K-bank was joined by KakaoBank – a subsidiary of Korea's leading messaging app and social network, KakaoTalk - the second entity awarded such a licence. Such banks are being encouraged to implement biometric authentication technology using iris, voice and facial recognition, creating potential collaboration opportunities for domestic and foreign InfoSec companies.

4.1.4 Case Studies – Finance Industry

Shinhan Bank	
Website	www.shinhan.com
Problem	How to make personal banking faster and safer?
Solution	Used biometric identification to access services
Who implemented it?	Internal security team with undisclosed 3rd party consultancy
Overview	Shinhan Bank, one of Korea's largest banks, is using biometric information to prevent hacking. In December 2015, Shinhan Bank introduced "Shinhan Your Smart Lounge", a self-banking counter using palm veins as biometric identification. During its first 15 months in service, it processed 350,000 transactions safely via 26 Smart Lounges. The bank expects to expand the range of services it offers through biometric identification in the near future.

Shinhan Card / Hana Card	
Website	www.shinhancard.com / www.hanacard.co.kr
Problem	How to detect fraudulent behaviour and theft of credit card details?
Solution	Used AI and Big Data-powered e-commerce Fraud Detecting Systems
Who implemented it?	Internal security teams in collaboration with Uplus IT, Interezen, SNU etc.
Overview	Credit card companies are bolstering their systems' protection against fraud. According to one market insider, Hana Card collaborates with security professionals from companies such as Uplus IT and Interezen to introduce 'eFDS' (e-commerce Fraud Detecting Systems). This technology generates device certification keys using data on an individual user's IP-address, browser, operating system etc. to identify the user when he or she is paying online. Also, Shinhan Card is setting up an FDS system using AI Deep Learning in co-operation with researchers from Seoul National University. This particular technology uses AI automatically to detect abnormalities which indicate fraudulent transactions.

With more fintech companies and traditional banks open to the idea of newer forms of security, this could be a potentially lucrative opportunity for UK companies in 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 and digital payment protection, as well as blockchain.

4.2 Information Security for Autonomous Vehicles

The rise of IoT is bringing about an increase in the type and number of connected products and one area that has received a lot of attention is the automotive sector. According to IHS Markit's estimate, over 112 million connected vehicles are running worldwide. With smart cars and connected cars seeming to be the future, the tiered suppliers and the automotive OEMs in Korea are focusing on the possibility of a cyber-attack on their vehicles. An example of this is Hyundai Mobis. To prepare for potential threats, this tier-one supplier has joined Auto-ISAC, a private consultative group that focuses on initiatives to tackle the latest cyber threats.

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

While the Korean vehicle IT security market is still nascent, the share of IT components in vehicles continues to grow quickly. Hyundai and Kia announced the addition of AI into their vehicles from 2019. In the same year, Korea's leading telecoms companies plan to commercially launch 5G, with connected vehicles seen as one core application. This mismatch between rapidly increasing IT security demand and limited local supply is a great opportunity for a UK company which specialises in automotive parts security to partner with one of the larger automotive vehicle makers in the world.

4.2.1 Case Studies – Autonomous Vehicles

Penta Security	
Website	www.pentasecurity.com
Problem	How to protect connected vehicles against hacking
Solution	Develop three-stage security solution for connected vehicles
Who implemented it?	IoT Convergence Security Research Center within Penta Security
Overview	Penta Security has developed a three-stage security solution for connected vehicles. The system complements hardware security provided by automotive semiconductor suppliers by adding a firewall-protected gateway as a first line of defence coupled with a Key Management System (KMS) protecting communication to the ECU as well as Penta Security's AutoCrypt solution which implements a Public Key Infrastructure (PKI) for external communication.

4.3 Information Security in Digital Health

The Korean healthcare system is unique in that, while hospitals in Korea are categorised as non-profit organisations, they are run more like companies. This means they actively compete to attract patients and are highly receptive to new technologies. The industry is dominated by a handful of large players which operate networks of branch hospitals. Over 80% of outpatients visit the top five hospitals: Seoul Asan Hospital, Samsung Seoul Hospital, Seoul National University, Severance Hospital and St Mary's Hospital. The dominance of a small number of large hospitals, coupled with Korea's advanced ICT infrastructure, facilitates the integration of new technology and makes the country an excellent test bed for new applications.

Along with the increased use of ICT in hospitals and medical research institutes, there is large demand for InfoSec solutions related to network security as well as data protection. For instance, the Korean government plans to select six major hospitals over the first half of 2018 to collect data from around 10 million people to create a biologic information database, while the National Biobank of Korea, a government-run research institution, aims to collect biospecimens from 500,000 participants in Korea. The creation of such databases poses an opportunity for UK companies, as the handling and security of this data will be paramount.

Digital health is not just a key sector for public institutions and the medical industry, it has also been identified as a growth sector by large enterprises. For example, Young Sohn, Samsung's Silicon Valley-based President and Chief Strategy Officer, stated that the company is focused on preventive health and related technologies. The market for digital health-related InfoSec solutions will grow concurrently, with opportunities particularly in authentication, data encryption, database protection, and medical IoT network security.

4.3.1 Case Studies – Digital Health

Catholic Medical Center (CMC) / Catholic University of Korea St. Mary's Seoul Hospital	
Website	www.cmcseoul.or.kr
Problem	How to increase patient data protection in the healthcare industry
Solution	Apply secure data encryption protocols to patient databases
Who implemented it?	CMC IT department and Symantec
Overview	In the early 2010s, St. Mary's Seoul Hospital, along with several other hospitals, came under fire due to reported cases of confidential patient information being used by unauthorised third parties (e.g. pharmaceutical industry marketers). In a competitive medical services market in Korea, the issue of patient data protection is key to patient retention, so CMC selected US-based Symantec Corporation to provide a solution. Cases such as this have prompted the government to invite leading medical and IT specialists to develop new unified patient data protection guidelines for Personal Health Record (PHR) systems and a new system architecture which is to be applied to the nationwide healthcare system.

4.4 Encryption Services

Constant cyber security threats, combined with the need of conglomerates to ensure that their business secrets are not compromised, mean the Korean data encryption platform market is growing quickly. Investments into the encryption market are expected to grow from GBP 36 million in 2015 to GBP 98 million by 2022. There is strong demand for solutions that can encrypt data within file systems and provide differentiated levels of access.

Currently, most data encryption providers in Korea are local companies including KSign (estimated 28% market share by revenue), CubeOne (18%) and Penta Security Systems (15%). The remaining 39% of the market is divided between large multinationals like Symantec, Microsoft and HP, as well as smaller local and overseas suppliers. Notably, KT DS, Korea Telecom's IT service solution affiliate, recently announced that it will be entering the global data encryption market with a new home-grown solution.

The type of encryption solutions commonly used in Korea has been shaped by the Personal Information Protection Act (PIPA). To comply with PIPA, many data encryption solutions used to be hardware-based and centred around an IT system's core, i.e. hard drives, servers etc., which resulted in a relatively slow adoption of cloud-based encryption services. However, concerns surrounding cloud-based encryption have since largely been addressed and secure cloud services are now growing quickly within the country.

4.4.1 Case Studies – General Encryption

SK Telecom	
Website	www.sktelecom.com
Problem	How to protect IoT network infrastructure against hacking
Key Technology	Develop quantum random number generator chip for IoT devices
Outcome	SK Telecom's nationwide IoT network has robust hardware encryption
Developed by	SK Telecom
Overview	Following the 2016 Mirai Botnet incident, it has become clear that the Internet of Things is not only a great opportunity, but also potentially a massive security risk. SK Telecom has responded to this issue by developing a Quantum Random Number Generator (QRNG) chip to protect its nationwide IoT networks (LTE-M, LoRa, LTE Cat.M1) through quantum cryptography. SKT developed a miniaturized, 5x5mm chip to integrate into IoT chipsets and developed a dedicated repeater to extend the encryption signal range to 120 km. The chip was released in July 2017 and has since been applied to SKT's nationwide IoT networks. Given that the Mirai Botnet attack did not strike at the network level, but affected end-user devices, SKT is also developing a USB-type QRNG to upgrade security on existing devices such as set top boxes.

4.5 Information Security in the Public Sector

The need to introduce adequate information protection is arguably more urgent in the public sector which has concerns about citizens' privacy and safety at its core. Three agencies are tasked with identifying, preventing and responding to cyber-attacks and state-level security threats: The National Cyber-Security Center, Korea Internet Security Agency (KISA), and the National Police Agency's Cyber Terror Response Center. Moreover, an institution of higher learning specialising in cyber warfare has been chartered, increasing the amount of government-employed security experts from 400 in 2014 to up to 5,000 by the end of 2017. Hackers have targeted government agencies in Korea, endangering the welfare of government officials and civilian employees alike. North Korea alone purportedly has more than 3,000 state-employed hackers specialising in cyber warfare and espionage.

The key areas of interest include encryption solutions, anti-malware solutions, DDoS attack protection solutions, cyber-threat detection solutions and consulting services. However, overseas companies may find themselves at a disadvantage in public procurement bids, so partnering with an experienced domestic InfoSec system integrator is recommended as the primary route to market. The process of obtaining certification can take six to 12 months and, because of the cost associated with obtaining Korea-specific certifications, companies should conduct a detailed cost-benefit analysis before moving ahead.

The typical public sector customers of information security technology companies include local governments, e.g. Seoul Metropolitan Government, Korea Immigration Service or National Tax Service. However, to address their needs, companies need to clear several hurdles.

4.5.1 Encryption Solutions for the Public Sector

The Korean government exhibits protectionist tendencies when it comes to encryption solutions. For example, the global encryption standard is the Advanced Encryption Standard or AES256, whereas the Korean public sector is required by law to purchase solutions with the ARIA256 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 ARIA256 or have registered with the government as approved suppliers.

“

Industry Insider's Thoughts

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

Sales engineer working for an international supplier of encryption services

4.5.2 Common Criteria Certification

Public institutions purchasing IT systems must procure systems that include security functions that conform to the requirements of the National Intelligence Service. This generally means 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.

The security conformance verification system consists of a verification organisation and a testing organisation. The National Intelligence Service, the official verification authority, accepts applications for verification of security conformity and supervises the management of the test work. The Korea Internet & Security Agency provides detailed guidelines on and support for certification procedures.

4.5.3 Case Studies – Public Sector

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	On December 23 2014, KHNP announced it had been hacked. Nuclear reactor blueprints, sensitive technical specifications and personal information of over 10,000 employees had been 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 co-ordinated 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. Multiple government agencies and private cyber security consultants were brought together to create a nationwide "cyber security control tower" inside of the National Security Office (NSO) to develop strategies to combat cyber-attacks effectively, foster technology adoption and educate government workers on personal preventive measures.

5. Market Entry Strategies

KEY POINTS

- Direct sales into the large conglomerates are possible but on-the-ground support is strongly advised
- Partnering with local systems integrators or value-added resellers is advisable for foreign companies as they know the market and can provide the after-sales support required in-country
- 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 products or services

Both the government and larger conglomerates are increasingly focusing their attention on the importance of information security. Because the InfoSec sector is still young and home-grown solutions are still catching up with global standards, Korean companies often rely on the expertise of global firms. Korea therefore offers many opportunities for UK businesses with cutting-edge InfoSec solutions.

While opportunities certainly exist, the Korean InfoSec market poses a number of challenges including a need for localisation, regulatory requirements and high expectations for responsive Korean-language customer support. British companies looking to enter the Korean market may find it advisable to seek local support or engage in a strategic partnership with a local business to navigate these obstacles. UK businesses can approach the Korean market either 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 InfoSec solution 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 a lot of documentation to be translated, but it will allow 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

In conclusion, the Korean InfoSec market offers strong opportunities to UK companies but, whichever option a UK company selects to enter the market, these and other business and cultural considerations must be addressed, and local support often proves invaluable in the market entry process.

For further information

Please contact:

Department for International Trade
Trade.Korea@fco.gov.uk

Michal Waszkiewicz
Director, Sales and Marketing, Intralink UK
michal.waszkiewicz@intralinkgroup.com

Jonathan Cleave
Managing Director, Intralink Korea
jonathan.cleave@intralinkgroup.com

www.intralinkgroup.com

Department for
International Trade

Intralink

great.gov.uk

DIT
The UK's Department for International Trade (DIT) has overall responsibility for promoting UK trade across the world and attracting foreign investment to our economy. We are a specialised government body with responsibility for negotiating international trade policy, supporting business, as well as delivering an outward-looking trade diplomacy strategy.

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.

© Crown copyright 2018
You may re-use this publication (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.
To view this licence visit:
www.nationalarchives.gov.uk/doc/open-government-licence
or e-mail: **psi@nationalarchives.gsi.gov.uk**
Where we have identified any third party copyright information in the material that you wish to use, you will need to obtain permission from the copyright holder(s) concerned.

Any enquiries regarding this publication should be sent to us at **enquiries@trade.gsi.gov.uk**

Published July 2018 by Department for International Trade.