# CYBER SECURITY MARKET OUTLOOK IN KOREA- Vol. I

# THE SECURITY MARKET SIZE IN SOUTH KOREA

*Unit: USD 1 billion*

| | 2018 | 2019 | 2020 |
|---|---|---|---|
| PHYSICAL SECURITY MARKET | 3.1 | 3.1 | 3.3 |
| CYBER SECURITY MARKET | 1.5 | 1.6 | 1.7 |
| DOMESTIC SECURITY MARKET | 4.6 | 4.7 | 4.9 |

*Source: BOANNEWS, Security World*

# SECURITY MARKET OVERVIEW

With a 5.2% increase, South Korea's Security Market size is almost on the verge of hitting approximately USD 5 billion this year and the domestic security market is estimated to have reached USD 4.7 billion last year, in which USD 3.1 billion belong to physical security and the rest (USD 1.6 billion) to cyber security.

ICT technology developments such as AI, IoT, Deep Learning, Big Data, and Autonomous driving, enable a more successful convergence of physical and cyber security. As security convergence is the trend of the current security industry, its development will enable the market to easily reach the target. The legal foundation which the Ministry of Science and ICT(MSIT) plans to lay, will eventually attract even more attention to this new trend. South Korea has rapidly developed into a highly technical country because many of its people realized the value in technological development and is now much more capable of responding to emergency security risks issues than it could have done previously. In many ways it is rightfully now recognized as a global leader.

Compared to 2018, the growth rate of physical security was slow, however, 2020 looks different. The vigorous development and demand for biometrics and access control foresees a much more dynamic growth compared to 2019. According to the public sector's 2020 security equipment and service purchase demand, a demand of 452 million dollars is predicted to occur. Cyber security market has also grown, where maintenance and consistent security service purchase demand rate has risen in large figures.

# CYBERSECURITY IN SOUTH KOREA

*Unit: USD 1 million*

| | 2016 | 2017 | 2018 | 2019 (est.) |
|---|---|---|---|---|
| **TOTAL MARKET SIZE** | 1,771.7 | 1,875.9 | 2,063.6 | 2,084.3 |
| **TOTAL LOCAL PRODUCTION** | 1,128.1 | 1,165.1 | 1,281.6 | 1,294.4 |
| **TOTAL EXPORTS** | 88.3 | 91.3 | 100.5 | 101.5 |
| **TOTAL IMPORTS** | 732.0 | 802.3 | 882.5 | 891.3 |
| **IMPORTS FROM THE US** | 554.4 | 607.6 | 668.4 | 675.1 |

*Source: Korea Internet and Security Agency (KISA), Korea Information Security Industry Association (KISIA)*

Known as an IT powerhouse, South Korea possesses the most convenient cyberspace environment, along with a world-class information and communications technology (ICT) and the related infrastructure. As cyberspace has become a crucial factor, the interconnection, convergence, and its complexity require stronger vulnerability management systems to keep its devices safe.

In the past, malicious cyber activities were mainly carried out by individuals or hacker groups, however, with the growing involvement of criminal and terrorist groups, cyber attacks are now being executed on a larger scale. This created a paradigm shift in the prioritization of homeland cyber security and importance of cyber security in South Korea.

Market demand for cyber security devices and services in South Korea has grown as the level of customer intelligence about security awareness has grown. According to the "2019 Domestic and Foreign Security Market Forecast", the market demand for cyber security in 2018 exceeded USD 2 billion representing 4.2 percent growth over 2017.

Market shares have been expanded in order to include next generation or superior capabilities such as Advanced Persistent Threat (APT) and next generation firewall solutions. Regardless of the firm sizes and solutions' countries of origin, Koreans have sought and are seeking the best-in-class and cutting-edge solutions to protect their systems from intensified cyber-attacks.

*Source: Export.gov and National Cybersecurity Strategy*

# MARKET TREND

According to IDC (International Data Corporation), Cloud's global market size has expanded from USD 78 billion (2015) to an estimated USD 277 billion (2021) at a Compound Annual Growth Rate (CAGR) of 23.1%. Such growth rate not only applies to the global market but also to the domestic market. At a Compound Annual Growth Rate (CAGR) of 16.8%, the demand for cloud computing will again be on the rise as its benefits are obvious- working environment changes such as cost saving for IT infrastructure management, business agility and the improvement of business efficiency.

However, cloud migration also has its consequences. Security and privacy are the two main challenges, in which the rise of cloud connectivity also implies a rise in the number of cyber attacks. As the attacks have become more elaborate, security systems have now become crucial irrespective of the IT environment. The current noteworthy type of cyber attack is the increase of new malware. 41% of the total observed malware have been identified as new types, where 70% of these new types have been created by open source tools. This indicates how the attacker is not only capable of updating the pre-existing malware, but also capable of inventing and applying malware which is able to circumvent detection.

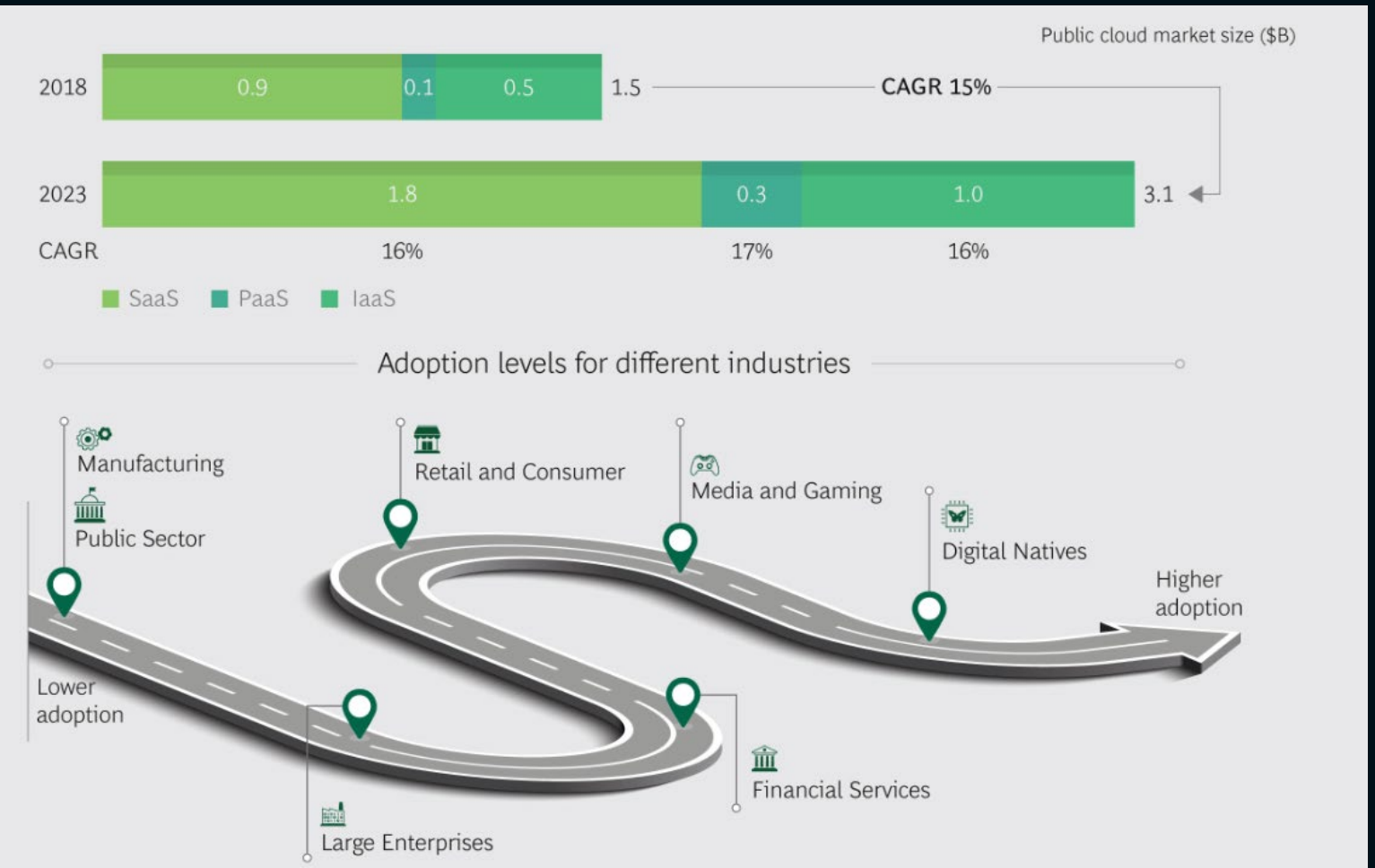
Ransomware attacks have been around for a while, but the attacks being carried out for financial profit is quite new. 29% of the attacks which were dealt with, were mainly financial exploitations and card theft. Next on the list is the intellectual property theft such as data theft, taking up 22% of the total number of attacks. As ransomware attacks are an easy job for cyber attackers and provides them with immediate financial benefits, it is foreseen that ransomware attacks will not be put to a halt in 2020.


One cannot discuss about the 4th Industrial Revolution without noticing cloud computing. A large number of companies, from start-ups to conglomerates, are rapidly incorporating cloud technology and even the government is strongly encouraging cloud migration, resulting into an intensified competition between companies for prior occupation of the market.

It was about 7, 8 years ago when public cloud first emerged in South Korea. Despite the many issues and problems, the cloud market is being revived thanks to its three advantages - flexibility, elasticity and cost reductions. It was for such reasons why the Korean game companies applied cloud computing before the service was officially available.

By securing computing resources on top of the existing public cloud, data centers were able to obtain a higher availability through auto scaling. The previously mentioned factors alleviate the burdensome staff expenses, expenses for data center establishment, operation expenses and investment costs. In addition, maintaining the availabilities of replication, back-up and DR (disaster recovery) have become much easier by infusing cloud computing. Thus, the customer is now able to identify business opportunities by using the right amount of the service provided. Such services can easily be applied to Big Data analysis and IoT, in which the act of customers having to form the entire framework is no longer necessary.

# PUBLIC CLOUD MARKET IN SOUTH KOREA
## (2018-2023)



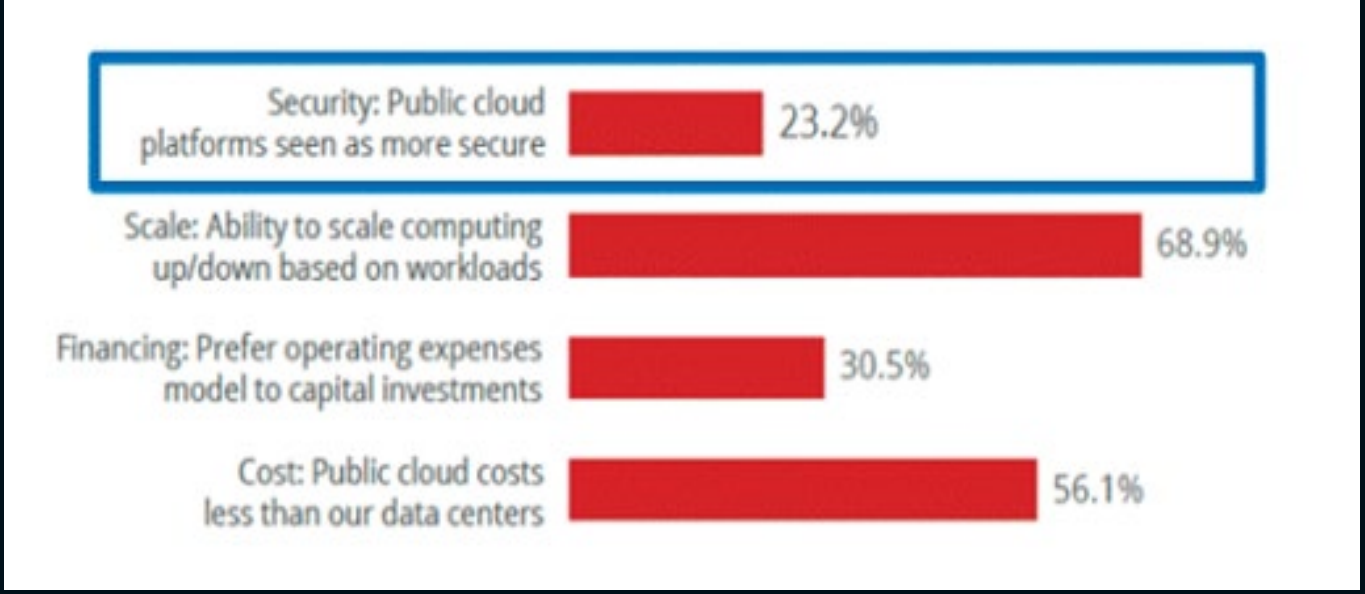

**Sources:** Expert interviews, Survey of public cloud users and decision makers (n=1026), Industry reports, BCG analysis
**Note:** SaaS refers to Software as a Service and includes business processes and support projects market, PaaS refers to Platform as a Service and IaaS refers to Infrastructure as a Service model; all CAGRs shown are 3 year CAGR for 2018-23

With a compound annual growth rate (CAGR) of 15%, South Korea's public cloud market is expected to reach USD 3.1 billion by 2023. The SaaS model is the largest and fastest growing segment, accounting for 45% of the market. IaaS is slowly gaining market share, and is expected to account for about one-third of the market by 2023.

Digital native businesses, along with media and gaming companies, are major spenders in South Korea's public cloud market. Online gaming, e-commerce, and other wholly digital businesses that need to deliver the best possible online experience can give their customers unprecedented speed, along with experimental games and features using augmented reality and virtual reality.

*Source: BCG- Ascent to the Cloud: How Six Key APAC Economies Can Lift-off*

# CHALLENGES FACING PUBLIC CLOUD




*Source: Reasons for using Public Cloud- CSA Cloud Security Alliance 2018*

Negative views on public cloud still exist. The uncertainty lies within the fact that the intelligent assets are stored in an external platform. Invisibility is the other reason. People normally feel relieved and certain about things which they can actually see, however, as the public cloud platform is not an object which is visible, many customers feel anxious about using the service. In order to reduce the anxiety, Korean cloud platforms such as NBP and NHN Entertainment are providing a 24 hour client service.

The discard of data is the other negative view on public cloud. As a solution, the 'tenant' by MS, grants access to the data platform only after the approval process, which applies to the manager as well. Secondly, in accordance with the national data regulations, the Data Residency system does not allow the data to be duplicated and sent out overseas. It is clear that security is the biggest concern and such is the reason why public cloud service enterprises are investing huge amounts into security systems.

# COUNTERMEASURES IN KOREA


**PUBLIC G-CLOUD**

- Korea's first company to have obtained the public cloud certification in 2016
- After 5 years of stable management, customers include 130 public institutions
- Financial security data center (FSDC)
- Emphasis on the importance of security


**NAVER CLOUD PLATFORM**

- 14 security certifications issued by KISA
- ISMS (Information Security Management System), PIMS (Personal Information Management System), CASP (Cloud Security Assurance Program) certifications
- CSA STAR (Cloud Security Alliance Security, Trust, Assurance and Risk) certification

**TOAST**

- Security across the whole infrastructure and additional security service chosen by the customer
- Security service provided by subsidiary security consulting company PIOLINK and DB security company PNPSECURE
- 24/365 service provided by the technical staff

In December 2018, the Korean government issued an official Public Cloud Guideline for all administrative agencies and public institutions. The main reason for the issue was to provide the institutions a safe and efficient way of using public cloud and to protect its domestic enterprises. The table below indicates how public cloud can be used for information systems but not for the central department and local governments' internal business systems.

| | Central Department | Local Government | Public Institution |
|---|---|---|---|
| **Information System (excl. internal business system)** | Public Cloud | | |
| **Internal Business System** | Public Cloud not allowed | | Public Cloud |

*Source: Ministry of the Interior and Safety Public Cloud Guideline*

Obtaining cloud security certifications before providing its services is absolutely crucial. However, obtaining the related security certification does take time and is not easy. In Korea, KT, NBP, NHN Entertainment, LG CNS and GABIA are the five domestic cloud service providers which fall under the category.

Public institutions in Korea are still unfamiliar with the public cloud service. But one cannot deny the fact that greater number of enterprises and institutions are considering the use of public cloud services. Therefore, it is beneficial to first choose a target in which public cloud services can easily be applied by stages rather than changing the system in one go. Whether the business service of an enterprise can be directly applied to the standard platform of public cloud, whether there is an internal staff in charge of managing public cloud and whether the security level meets the needs of the business service, are all factors to consider before using public cloud services.

# HYBRID CLOUD

Instead of using public cloud on its own, Multi and Hybrid Cloud are the new trend. Multi cloud not only makes use of one single public cloud, but a number of public clouds, managing to operate both hybrid and public cloud. Major companies have already invested a huge sum into their essential data legacy systems. Instead of replacing their legacy with public cloud, many major companies are using private cloud systems on top of their basic legacy systems whilst managing their new systems on public cloud.

As an example, NHN Entertainment are concentrating on an IaaS strategic roadmap suitable for both cloud services. Their target is creating a flexible cloud service meeting the specific needs of customers.

KT is currently expanding the industry market through their E2E cloud, concentrating on the SI market and multi cloud based markets. The new VMware Cloud supports the standard Private Cloud system and its migration, expansion of Hybrid Cloud, and DRaaS service.

# CASE STUDY
# PUBLIC CLOUD

CASE STUDY

## LG CNS

INDUSTRY
MANUFACTURING

### ABOUT THE COMPANY

LG CNS is a subsidiary of LG Corporation and is one of the largest IT service providers in South Korea.

### CHALLENGE

LG Chem with the help of LG CNS, needed support for harnessing advanced technology to improve model accuracy for a glass substrate used in LCD TV manufacturing. Previously, inspection of the models was labor intensive and time consuming, with 5-6 quality inspection processes for every production line.

### Internet of Things, artificial intelligence and edge computing save time and labor on the factory floor

LG Chem with the help of LG CNS, uses Edge IoT Core to run cloud-trained machine learning (ML) models for defect detection to process images across thousands of machines.

1 Junior engineer **takes 2-9 hours** to perform modeling, achieving **99.9% accuracy** in glass inspection

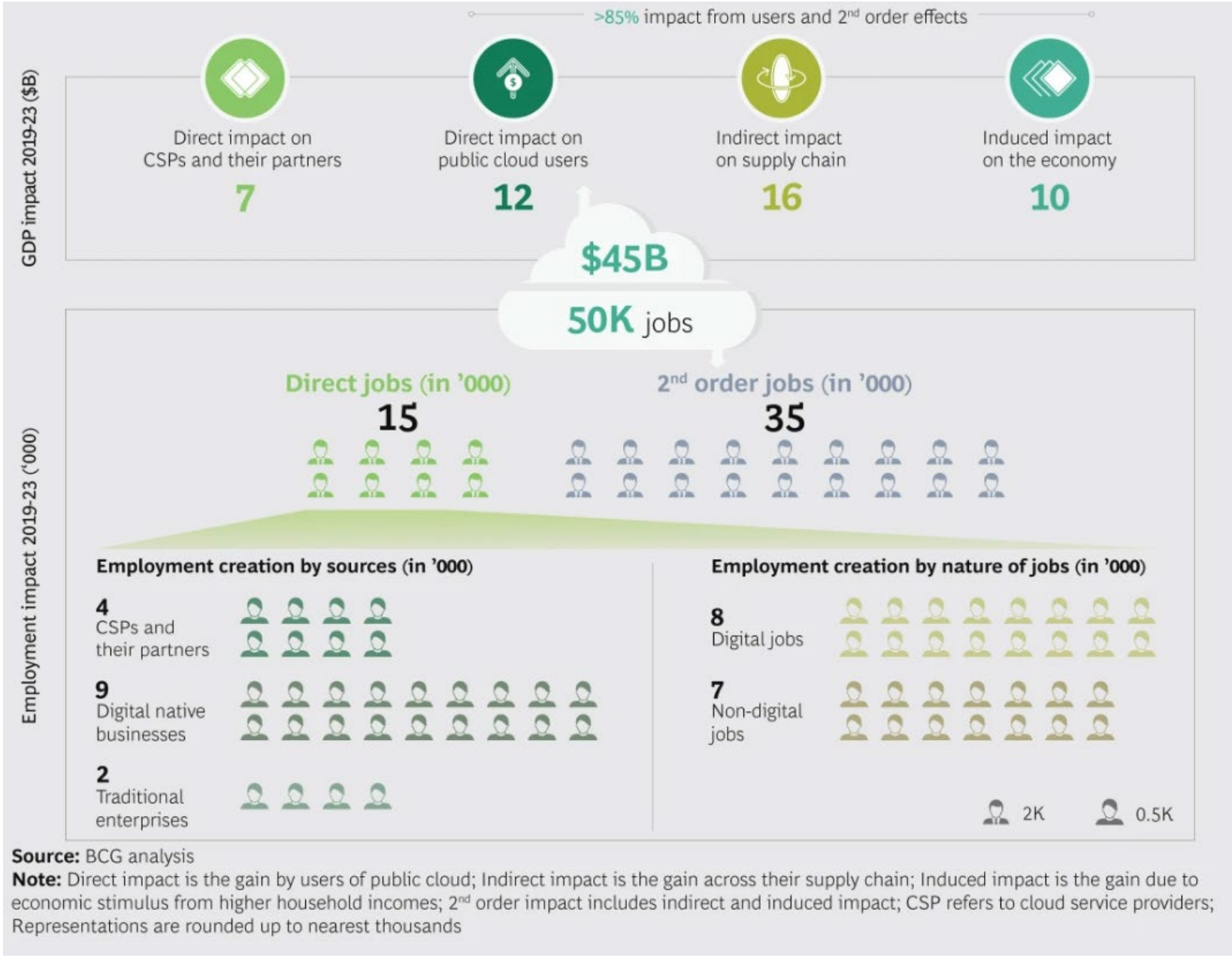
**The public cloud saves** about **$1M per year per production line**

**Deep learning models are run locally through** computer vision system

*Source: BCG- Ascent to the Cloud: How Six Key APAC Economies Can Lift-off*

# THE ECONOMIC IMPACT

## Public Cloud is expected to drive cumulative GDP impact of $45B and total employment impact of 50K jobs over 2019-23 in South Korea




**Source:** BCG analysis

**Note:** Direct impact is the gain by users of public cloud; Indirect impact is the gain across their supply chain; Induced impact is the gain due to economic stimulus from higher household incomes; 2nd order impact includes indirect and induced impact; CSP refers to cloud service providers; Representations are rounded up to nearest thousands

# THE ECONOMIC IMPACT

The overall cumulative economic impact from direct, indirect and induced sources is expected to be USD 45 billion (KRW 54 trillion), if CSPs continue to launch new products and services at their present rate, and policymakers keep their existing stance on public cloud deployment. When annualized, this is equivalent to roughly 20% of the annual impact from large traditional sectors such as the automotive industry, about 10% of the annual impact of the electronics industry, and about 0.6% of the country's annual GDP.

About 85% of the total impact will be generated within user verticals, while around 15% of the impact will come from the growth of cloud service providers and the IT industry. Of the direct gains to industry, a major percentage will come from enhanced business revenues. A total of USD 10 billion (KRW 12 trillion) will come from revenue uplift, while another USD 1.3 billion (KRW 1.5 trillion) will result from productivity benefits, and USD 0.5 billion (KRW 0.5 trillion) from IT-related cost reductions. Half of the total impact is expected to come from the industries that have been the big spenders on the public cloud—digital native businesses, especially those in retail, along with media and gaming companies and select chaebols driving public cloud within their businesses.

Public cloud usage stands to create close to 15,000 direct jobs over the next five years. Roughly 7,000 of the direct jobs will be in non-digital roles such as sales, marketing, human resources, finance, logistics and operations. Another 8,000 will be digital jobs, of which an estimated 4,000 will be with cloud service and IT system providers and the remaining 4,000 will be with industry verticals—representing approximately 1% of the current information and communications technology workforce.

The second order effects are expected to influence another 35,000 indirect and induced jobs, bringing the total potential jobs that are offshoots of public cloud use to 50,000. That is equal to about 0.4% of the current workforce. A large proportion of these jobs will likely be taken up by the existing workforce after their retraining and upskilling.

*Source: BCG- Ascent to the Cloud: How Six Key APAC Economies Can Lift-off*

*"Users are interested in adopting the public cloud less for the benefits of the actual cloud migration such as cost saving, but more for the fact they can more freely and easily try out additional services such as AI, big data, and analytics."*

*-Director, ICT accelerator*

***Despite the negative views on the application of Public Cloud, the service is definitely on its way of becoming the main trend. As a response to the 4th Industrial Revolution, the Korean government is encouraging many to effectively use this service. It is foreseen that the domestic public cloud market is to grow rapidly every year, in which the competition between its service providers are unfolding in an intense manner.***

# MARKET TREND
## SECURITY CONSULTING

According to the survey conducted by IBM in April 2019, 77% of the 3,600 IT professionals and 54% of GDPR enterprises did not have any specific Incident Response Plans. 70% of the respondents explained how there just aren't enough number of staff capable of supervising the incident responses and 48% of the enterprises expressed how the large number of security tools make security management harder to handle. Such responses eventually lead to many cyber threats and the clear fact that creating an Incident Response Plan is almost impossible without professional assistance. Is there a way to overcome such dilemma? The answer is YES.

Consulting and giving professional advice to the public or to those practicing the profession also exist in the field of security. 'Security Consulting' is a service which protects the customer's intelligence assets by analyzing the threat/dangers, setting up feasible countermeasures and materializing them.

# TYPES OF SECURITY CONSULTING


*Source: IGLOO Security*

| Information Security Consulting | Personal Information Protection | Personal Information Influence Evaluation | Certification Consulting | Communication Infrastructure Consulting | Vulnerability Inspection Consulting | SOC Consulting |
|---|---|---|---|---|---|---|
| An overall information security master plan containing an analysis on information protection statuses and security issues of customer companies based on the latest information protection acts and standard. | Improvement measures based on the analysis on personal information processing status and personal information protection issues of customer companies based on latest personal information protection laws and standards. | Improvement measures based on the analysis on management of personal information processing system and personal information protection issues of customer companies by focusing on influence evaluation and latest personal information protection laws. | Protection measures to risks deduced from status analysis based on inspection items required by each certification, providing consulting service to all processes from preparation to acquisition of certification by supporting document condition preparations such as implementation evidence required for certification procedures. | Consulting for major information communication infrastructure as well as identification and classification of asset, diagnosis of vulnerabilities of information system, (server, network, DBMS,WEB, PC, etc.) diagnosis of vulnerabilities of web application (simulated hacking) and the analysis of degree of risk. | Diagnosis on technological weaknesses regarding major information systems (server, network, DBMS, information protection system, etc.) operated by customers and proposes protection measures to deduced threats to improve security and decrease the risk of occurrence of incidents. | Security Operation Center (SOC) can be an essential task for the cyber security in order to provide enhanced security and rapid response to security events throughout the network. SOC will be designed in the manner that optimally utilizes and draws out the performance of the equipment and the characteristics of heterogeneous security devices. |

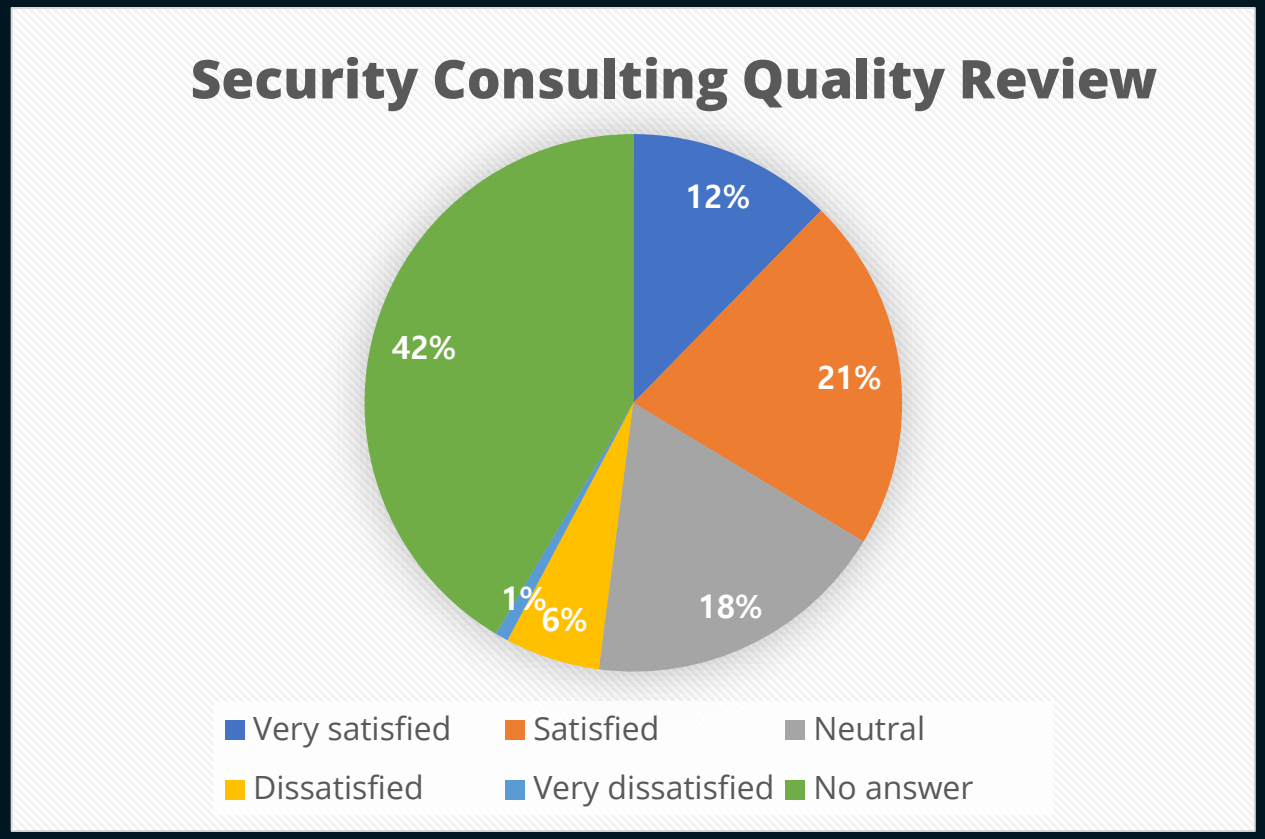
*Source: IGLOO Security*

# MARKET SIZE

According to the <2020 Domestic and Global Security Market Outlook> released by BOANNEWS and SecurityWorld, the market size of security consulting was valued approximately at USD 91 million and is foreseen to grow from USD 95 million in 2020 to USD 98 million by 2021. The global security consulting market, according to Markets and Markets, is estimated to reach USD 26 billion by 2021 with an annual growth rate of 10.2%. The use of third party applications, M&A, the increasing number of overseas expansions, complex network, the proliferation of IoT and BYOD, and sophisticated cyber attacks are the main causes of the market growth.

In 2001, the security consulting industry in Korea started off with only 9 enterprises designated as professional companies of intelligence. 100 security consulting enterprises currently exist in which 20 of them are designated as professional companies of intelligence- SECUI, AhnLab, eNsecure, A3SECURITY, LOTTE Data Communication, CYBERONE, SK infosec, PIOLINK, SOMANSA, CAS, SSR, FASOO, WINS, IGLOO Security, SecureOne, EY, KEPCO KDN, Shinhan DS, KTIS, and F1Security. Out of the 20, the five leading security consulting enterprises are AnhLab, PIOLINK, FASOO, WINS, and IGLOO Security.


*Photo: State Security & Protective Services (Aust)*



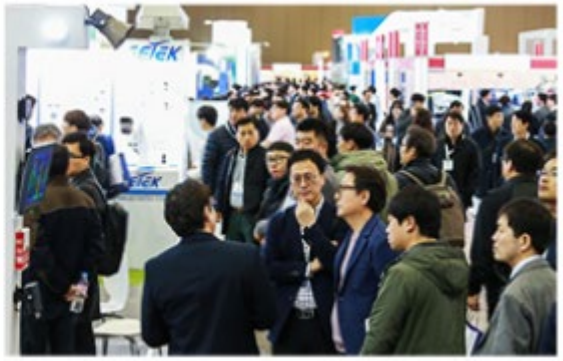

*Source: BOANNEWS and SecurityWorld*

BOANNEWS and SecurityWorld conducted a security consulting service satisfaction survey of 1,220 readers. 56.1% of the total number of readers have had the chance to receive the service, in which 33.6% have been satisfied.

The main reasons for those who refused the service (41%) was budget deficit and staff shortage. Many consider the service as 'not necessary' and 'not effective enough'- still regarding security just as an 'additional cost item'. However, there still is hope as 69.2% of the total readers are considering receiving security consulting services within the next three years.

*Visit www.seconexpo.com for more INSIGHT ON THE CURRENT SECURITY TREND*
*PRE-REGSITER to GET INSPIRED*

| | |
|---|---|
| Date | 6(Mon) - 8(Wed) July, 2020 |
| Venue | Hall 3~5, KINTEX, Korea |
| Organizer | SECON 2020 Organising Committee |
| Fair Manager | media. \| informamarkets |
| Official Media | BOANNEWS Security World |




## Contact our team for more information

**Ms. Kahyun (Susanna) Kim / MARKETING**
**E-mail: Kahyun.Kim@informa.com**
**Tel. +82-2-6715-5421**