UK-APAC Tech Growth Programme

Northeast Asia's cybersecurity market – opportunities for UK companies

February 2025

Intralink

Funded by UK Government

Contents

Executive summary

Japan, South Korea, and Taiwan present strong market entry opportunities for UK cybersecurity companies due to rising cyber threats and digital transformation across critical sectors like manufacturing, automotive, and healthcare. There is high demand for advanced solutions in cloud security, AI-driven threat detection, and industrial control systems, with significant growth potential in each market.

Japan

Japan's cybersecurity market is ranked 16th globally. It was valued at GBP 5.27bn in 2024 and is expected to reach GBP 6.2bn by 2027. Japan is experiencing a significant rise in cyber-attacks prompting urgent cybersecurity measures across critical sectors. Trends such as AI, increased use of cloud and IoT, remote work and society 5.0 are driving the need to enhance cybersecurity. There are challenges, including low investment levels, a severe workforce shortage, and outdated systems, particularly among small and medium-sized enterprises. The need for greater public awareness and better coordination between government and the private sector is essential to enhance Japan's cybersecurity posture and comply with international standards.

Japan is heavily reliant on foreign cybersecurity technology and the main areas of opportunity for UK cybersecurity companies are in IT and telecommunications, manufacturing, automotive and healthcare. Banking and defence also represent opportunity areas.

Opportunities in IT and telecommunications are driven by wider adoption of cloud and the increasing need for protection against AI-generated attacks.

Increased use of cloud, IoT, AI and automation in manufacturing are driving the need for cybersecurity, and Japanese companies are finally starting to take proactive steps in deploying OT cybersecurity solutions.

Connected cars, autonomous vehicles and ADAS are driving increased investment in cybersecurity in the automotive sector, and technologies of interest include security for V2X communication, intrusion detection systems, AI-driven threat detection and protection against future quantum threats.

Increased adoption of digital technologies in the healthcare sector (still heavily reliant on legacy systems) drives the need for solutions like encryption, advanced threat detection and response, data and access management.

Entering the Japanese market requires patience and a long-term view. Sales cycles are on average six to 12 months longer than in other markets and evaluation of technology is an extensive and exhaustive process. Consensus-based bottom-up decision-making and the language barrier are additional factors to consider. Since the COVID-19 pandemic Japanese companies are more open to online meetings, however, some presence in Japan is required to convert opportunities and in-country technical support is often a necessity. Exploring opportunities in Japan can initially be done by working with agents and distribution partners, but long-term commitment may involve setting up a local entity. To ensure the effectiveness of a channel strategy it is preferable to have a sales agent or an in-country employee.

Korea

South Korea's cybersecurity market is estimated to be worth GBP 4.06bn in 2024. The industry is projected to develop at a compound annual growth rate (CAGR) of 14.70% between 2024 and 2032 to reach nearly GBP 12.15bn by 2032. As one of the most advanced markets globally in terms of digitalisation, Korea continues to build out its digital environment across both the private and public sectors. However, due to this high level of connectivity, the country inevitably faces an ever-increasing number of cyber threats.

Cloud security solutions specifically have shown strongest growth over the last couple of years across the private and public sectors as both sets of organisations have been migrating their operations to the cloud, particularly after the COVID-19 pandemic. The pandemic pushed Korean enterprises and governments to accelerate the digital transformation and to make more everyday activities possible to achieve remotely.

In September 2023, the Ministry of Science and ICT (MSIT) announced the 'Strategy to Secure Global Competitiveness in the Information Security Industry' to grow the domestic information security market to a value of GBP 17bn by 2027.

Within that figure, it aims to grow the cybersecurity market to GBP 6bn, in part by enabling more domestic cybersecurity unicorns to develop. In the meantime, the market also welcomes international collaborators, as there is a strong need for technical expertise and commercial opportunities within and outside of the country.

Some of the areas of opportunity for UK cybersecurity companies are in automotive, manufacturing, IT and telecommunications, as these sectors tend to be targeted by cyber-attacks the most. Although the industrial infrastructure offers a wide range of potential end users, the Korean regulatory framework has a complex process for product/service certification thus, it is recommended to explore and essentially enter the market with the local partner already well established in the space. The UK's strong capabilities in threat intelligence and training would be the key component Korean cyber security companies would be interested in.

Taiwan

Taiwan's cybersecurity sector is on a strong growth trajectory, with 2024 revenues expected to reach GBP 628m and climb to GBP 785m by 2027. This upward trend is driven by the increasing complexity of cyberattacks and government support for a secure digital environment. Notably, cybersecurity solutions, encompassing software and hardware, are predicted to generate GBP 349m in 2024, while security services, covering areas like consulting and incident response, are projected to reach GBP 279m.

Taiwan's dominance in the semiconductor industry, and accounting for over 80 percent of global electronic manufacturing services (EMS), means cybersecurity is of the utmost importance. This is exemplified by TSMC, the world's largest semiconductor foundry, which has been a frequent target of malware attacks.

The Taiwanese cybersecurity landscape features prominent players like Trend Micro. In addition to established companies, a vibrant ecosystem of SMEs and startups is emerging, including TXOne Networks specialising in operational technology (OT) security and JmemTek providing hardware-based security solutions.

Significant opportunities exist for international collaboration, particularly with the UK. While Taiwan is involved in industrial control systems security and IC-based chip hardware security, the UK can contribute expertise in areas such as threat intelligence and cybersecurity training. The rise of sophisticated cyberattacks, suspected to originate from China, target Taiwan's critical infrastructure, including government networks and the semiconductor industry. This has created a surge in demand for advanced cybersecurity solutions.

Collaborations with Taiwanese cybersecurity companies and engagement with industry associations such as the Taiwan Information Security Association (TWISA) offer pathways for UK companies to enter the market. Participation in annual events like the CYBERSEC Taiwan and Cloud Taiwan conferences, as well as direct engagement with public agencies like the National Security Bureau (NSB) and the Administration for Cyber Security (ACS), can also facilitate market entry. Gorilla Technology, a provider of AI-powered video analytics and cybersecurity solutions, serves as a successful case study, having secured major projects in Taiwan, including collaborations with airport authorities and law enforcement agencies to enhance security and surveillance capabilities.

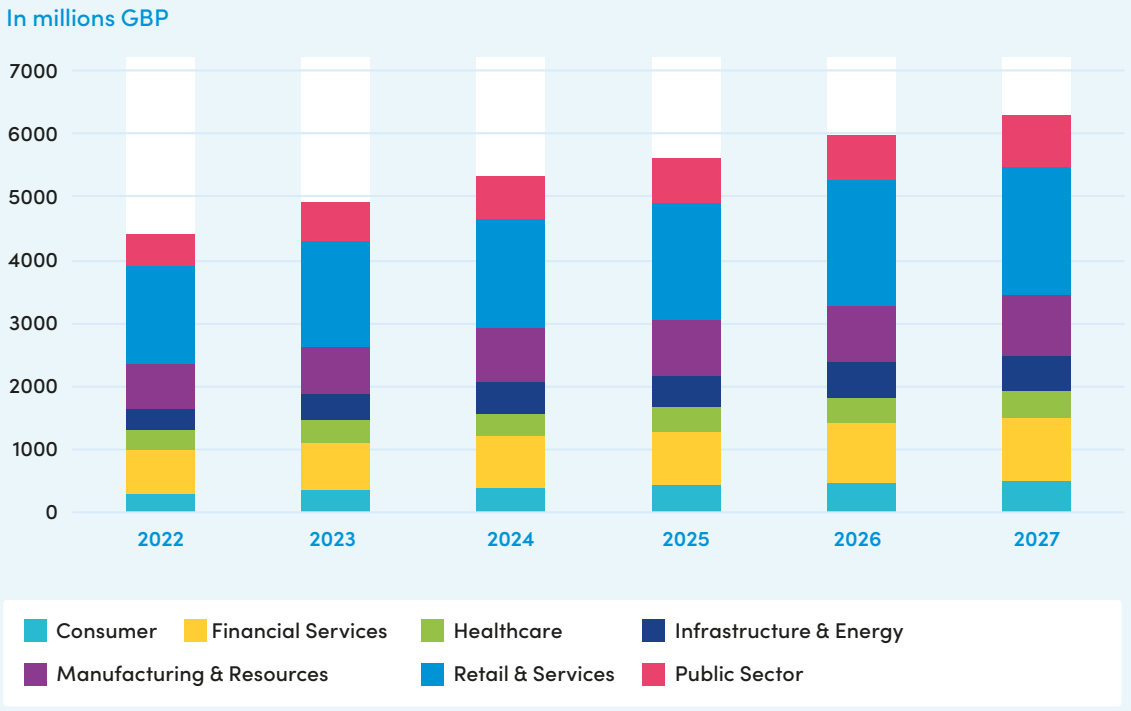
Japan's cybersecurity market

Market overview

Size of the market

Japan is the 16th largest cybersecurity market globally. While Japan lags the UK, which ranks third, growing awareness of the importance of cybersecurity is leading to increased investment in the public and private sectors. DIC Japan estimates the size of the Japanese cybersecurity market to be JPY 1.05tn (GBP 5.27bn) in 2024, a 7.6 percent increase from 2023 and the first time it will have exceeded JPY 1tn (GBP 5bn). By 2027, the domestic cybersecurity market is expected to reach JPY 1.25tn (GBP 6.2bn) with a CAGR of 7.2 percent. In 2023, cybersecurity services made up around 60.3 percent of the domestic market share, and the remaining 39.6 percent was for cybersecurity products.

Japanese cybersecurity market by business sectors



Source: IDC 2024

Market trends

The number of cyber-attacks targeting Japan, especially from overseas actors, is increasing. Critical infrastructure, government systems, and corporations are prime targets of ransomware attacks, putting national security and economic stability at risk. According to the deputy director of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the number of cyber incidents from abroad increased from 150 cases in 2021 to 230 cases in 2022 and continued to rise in 2023. The Ministry of Internal Affairs and Communications (MIC) reported an increase in cyber-attack related communications from 216.9bn packets in 2018 to 518bn packets in 2021, a 2.4 increase over three years. This comes as international guidelines for critical infrastructure's cybersecurity evolve and Japan tries to keep up with international standards.

The following trends are driving the growth in deployment of cybersecurity measures in Japan:

- **Artificial Intelligence (AI) –** rapid adoption of AI is bringing complexity and requires new measures to address such threats as AI-based spear-phishing and business email compromise (BEC) scams. AI is also being integrated to enhance response mechanisms to cyber incidents, improving threat detection and automation.
- **Increased use of cloud –** approximately 70 percent of Japanese companies currently use cloud. Japanese companies are making investments in identity and access management (IAM), encryption, and security information and event management (SIEM) to secure cloud environments, especially for IoT.
- **Increased use of IoT –** the number of IoT devices has increased from 23.1bn in 2019 to 39.9bn in 2024. The government is pushing for enhanced cybersecurity measures for IoT devices to protect against vulnerabilities as cyberattacks rise.
- **Society 5.0 –** as connected cars, smart factories, digital healthcare and other IoT technologies become more common, and the systems become increasingly interconnected, the need for cybersecurity measures is rising.
- **Remote work –** which has become common because of the COVID-19 pandemic, require additional security. Japan is starting to adopt a zero-trust security model with strict identity verification and access controls.

Challenges

Japan is behind other countries in the deployment of cybersecurity services and products. A 2023 survey by Assured showed that only 32 percent of Japanese companies are investing more than JPY 50m (GBP 0.25m) in cybersecurity, compared to 71 percent of American companies.

One of Japan's primary issues is a severe shortage of cybersecurity professionals, compounded by an aging workforce, limiting the country's ability to effectively defend against cyber threats. In 2023, Japan's workforce gap for cybersecurity was 110,254, a 97.6 percent increase from the previous year. There is also a lack of awareness and education among the public and even cybersecurity employees. Experts predict that AI will take over within the next few years, but many cybersecurity professionals admit that are still unfamiliar with AI.

Additionally, many companies, particularly small and medium-sized enterprises, are slow to adopt advanced security measures, often relying on outdated systems. This is due to limited budgets, traditional corporate cultures that often resist rapid change, and low public cybersecurity awareness.

There is an increasing pressure for Japan to comply with international regulatory frameworks such as ISO 27000 but lack of coordination between the government and the private sector is weakening cybersecurity defence strategies. Compared to overseas, Japanese companies are behind in the implementation of cybersecurity measures, for example, for third-party certification, the acquisition rate of SOC2 is over 50 percent overseas but less than ten percent in Japan.

Public sector initiatives

The main government organisations that regulate and contribute to cybersecurity in Japan are the Ministry of Economy, Trade and Industry (METI), the Ministry of Land, Infrastructure, Transport and Tourism (MLIT), the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and the Information-technology Promotion Agency, Japan (IPA).

Japan first introduced a cybersecurity law - The Basic Act on Cybersecurity - in September 2014. The purpose of the Act was to ensure cybersecurity whilst maintaining the distribution of free information.

The Act focused on voluntary cooperation between the government and private sector and established the Cybersecurity Strategic Headquarters to develop national cybersecurity strategies for business practices. The Basic Act on Cybersecurity led to the development of the Cybersecurity Management Guidelines (CMG), first introduced by METI in 2015. The CMG established that companies have responsibility for mitigating cybersecurity risks. The guidelines went through several revisions and the update in 2023 included the enhancement of cybersecurity management given the rise of cybersecurity threats and the increase in the use of cloud. One of the changes was an emphasis on implementing measures throughout the entire supply chain.

Name of organisation	Role
Ministry of Economy, Trade and Industry (METI)	METI is responsible for developing and implementing cybersecurity policies and guidelines, such as Cybersecurity Management Guidelines for Japanese Enterprise Executives and Cyber/Physical Security Framework
Ministry of Land, Infrastructure, Transport and Tourism (MLIT)	MLIT does not specifically focus on cybersecurity, but it can influence the cybersecurity space related to industries it oversees. For example, MLIT made the automotive industry harmonise its cybersecurity measures using a cybersecurity management system certification
National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	NISC is responsible for formulating Japan's cybersecurity strategy, reporting incident response and promoting international cooperation
Information-technology Promotion Agency, Japan (IPA)	IPA drives IT initiatives for the Japanese Government and is responsible for driving innovation in the IT sector, supporting government IT policies and providing cybersecurity guidance and training

As of June 2022, critical infrastructure is encouraged to comply with the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP) - critical infrastructure should strengthen its cybersecurity incident response systems, develop safety principles, reinforce information-sharing systems with cybersecurity-related organisations, utilise risk management and enhance protection infrastructure.

In Japan's attempts to align with international regulations, the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) introduced the ISMS conformity assessment system to certify whether a company's information security management system (ISMS) is consistent with international standards. Under this system, examinations are made to assess whether a company conforms with JIS Q 27001 (ISO/IEC 27001).

Japan's Ministry of Internal Affairs and Communications (MIC) established ISMAP (Information Systems Security Management and Assessment Program) in 2020, a cybersecurity certification framework designed to ensure that cloud services and other information systems meet stringent security standards.

The program incorporates Japanese and international security standards, and certification ensures systems are secure against potential threats and vulnerabilities.

Below is a summary of regulations in Japan that are applicable to cybersecurity solutions and services:

1. **Basic Act on Cybersecurity (BAC) –** basic framework for the responsibilities and policies of the national and local governments
2. **Telecommunication Business Act (TBA) –** ensures confidentiality of communications
3. **Act on the Protection of Personal Information (the "APPI") –** a principal data protection legislation
4. **The Japanese Foreign Exchange and Foreign Trade Act (FEFTA) –** regulates export of sensitive goods and technologies, including encryption software and hardware
5. **New Security Clearance Legislation (Japan's Economic Security Promotion Act (ESPA) –** protects sensitive information related to critical technologies and infrastructure, including cybersecurity
6. **The Unauthorised Computer Access Prohibition Act –** criminalises unauthorised access to computer systems
7. **The Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (also known as the IT Basic Law) –** determines the responsibilities of the government and local public entities, establishing the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society and initiating the development of a Priority Policy Program

International collaboration is key to Japan's cybersecurity strategy. The government is promoting coordination with international cybersecurity organisations which extends to sharing policy trends through multilateral frameworks like the G7 and bilateral meetings, as well as providing capacity building support to Pacific Island countries.

Japan is actively involved in the Quad Security Dialogue - a collaboration between Japan, the US, Australia, and India to address regional cybersecurity challenges and enhance information sharing which was established by Prime Minister Shinzo Abe in 2007 and revived in 2017 during the ASEAN Summits in Manila.

Japan also has separate dialogues with the US and the UK. The Japan-UK bilateral cybersecurity dialogue held its eighth meeting in September 2024 exchanging views on cybersecurity strategy and policy, international cooperation (including with the UN), and cybersecurity capacity building.

Japan also plays a role in the Forum of Incident Response and Security Teams (FIRST), to work with global incident response teams to improve collective cybersecurity practices, engages in the International Women's Cybersecurity Network (IWWN) to support and promote diversity in the global cybersecurity workforce, and contributes to advanced research and development on cyber threats and solutions through the Cybersecurity Research Institute (CRI).

International collaboration is key to Japan's cybersecurity strategy. The government is promoting coordination with international cybersecurity organisations which extends to sharing policy trends and providing capacity building support to Pacific Island countries.

Key players

The Japan market is reliant on foreign cybersecurity technology but also has its own strong players such as Fujitsu, NEC, IIJ and Hitachi. The share of foreign-owned companies in the cybersecurity products market exceeded 50 percent in both 2021 and 2022 according to a survey by IDC Japan.

Cybersecurity ecosystem

Regulators

MLIT Ministry of Land, Infrastructure and Transport

NISC

IPA 独立行政法人情報処理推進機構 Information-technology Promotion Agency, Japan

METI Ministry of Economy, Trade and Industry

Large companies

CISCO

IBM

FUJITSU

NEC

IIJ Internet Initiative Japan

Startups

SecureNavi

SPIDER AF

TRUSTDOCK

KEKKAI

CAULIS

HENNGE

Large companies

IBM Japan

IBM Japan is one of the largest players in the Japanese cybersecurity space with revenues of JPY 730.9bn (GBP 3.67bn) in 2023. IBM Japan offers a wide range of hybrid cloud, AI integrated, and customisable cybersecurity solutions. One of IBM Japan's main USPs is that it focuses on custom software development. To combat the lack of cybersecurity professionals, IBM Japan trains local RPG engineers and recruits skilled software engineers from abroad.

Fujitsu

Fujitsu is a major Japanese multinational information and communications technology (ICT) company. Fujitsu offers a range of services and solutions focusing on five key technologies: computing, networks, AI, data & security, and converging technologies. Fujitsu had consolidated revenues of JPY 3.7tn (GBP 18.6bn) for the year ending March 2023. Fujitsu is currently expanding into Australia and New Zealand with its launch of a new Cyber Security Services division in both countries in April 2024. Fujitsu continues to be a highly regarded company and is enrolled in the prestigious Microsoft Intelligent Security Association (MISA), an elite ecosystem of about 300 selected security partners recognised for their expertise and innovation in creating robust security solutions.

NEC

NEC is a major Japanese multinational information technology and electronics corporation that was established in 1899. NEC's revenue for the year ending March 2023 was JPY 3,313bn (GBP 16.6bn). NEC offers a wide range of products and services, and its recent areas of focus include cloud computing, AI, and IoT platforms. NEC offers a wide range of cybersecurity services across a range of industries, including network security implementations (firewalls, intrusion detection, etc.), security assessments and consulting, incident response and analysis, security monitoring and operations support, secure system design and implementation, compliance assistance and training programmes for customers.

In February 2024 NEC announced an alliance with Securonix to enhance its cybersecurity services in Southeast Asia. This partnership will improve NEC's cyber defence capabilities by integrating Securonix's advanced Unified Defence Security Information and Event Management (SIEM) technology into NEC's Managed Services Business Unit. The collaboration will provide enhanced visibility, cost reduction, and swift response capabilities.

Internet Initiative Japan (IIJ)

IIJ is a Japanese telecommunications company that was established in 1992. IIJ's revenue for the FY2023 was JPY 276.1bn (GBP 1.39bn).

IIJ was Japan's first internet service provider offering internet connectivity and WAN services, network-related services, cloud computing, systems integration services, network systems construction, operation, and maintenance, and development and sales of telecommunication equipment. IIJ offers a variety of cybersecurity services including a zero-trust platform called "Safous" which won the 2024 Cybersecurity Excellence Award for best zero trust solution. Other cybersecurity services include a cloud-based service offering security for corporate email and a Cybersecurity Awareness Training Program for employees.

Cisco Japan

Cisco established its Japan subsidiary, Cisco Japan, in 1992. It remains a mainstay in the market with seven offices spread throughout the country despite a six percent year-on-year decline in revenues in 2023. Cisco Japan offers a range of cybersecurity solutions including Zero Trust Security, Cisco Talos Intelligence for threat insights, a Cybersecurity Center of Excellence, Cyber Vision for operational technology security, Managed Security Services, and training programs through the Networking Academy. In June 2024, Cisco announced the establishment of its Cybersecurity Center of Excellence in Tokyo. This centre aims to enhance Japan's cybersecurity defences and digital resilience by focusing on appointing a National Cybersecurity Advisor, deploying the Cisco Talos Intelligence team, and training an additional 100,000 IT and cybersecurity learners over the next five years.

Startups

SecureNavi

SecureNavi offers an information security management (ISMS) and privacy mark (P Mark) automation tool. Its software enables companies to streamline security compliance by automating the handling of documents usually processed in Word and Excel. SecureNavi secured JPY 130m (GBP 0.65m) and JPY 460m (GBP 2.31m) at Pre-Series A and Series A respectively, with backing from Mobile Internet Capital and SBI Investments. SecureNavi won the ASPIC Cloud Award at the Venture Grand Prix in 2023.

Kekkai

Kekkai offers a Web3 security tool that protects cryptocurrency assets through simulation analysis and warnings about potential phishing activity. Offering a dashboard, mobile app, and plugin tool, Kekkai is already used by over 30,000 active users, covering over a million monthly transactions and GBP 152.1m in assets. Kekkai raised JPY 230m (GBP 1.16m) in seed funding with support from Stratified Capital, Sora Ventures, and Plug and Play.

Trustdock

Trustdock offers digital identity verification and know your customer (KYC) solutions. It provides a digital ID wallet application that enables eKYC, including authentication of the My Number Card, and an API infrastructure service for KYC. Trustdock enables users to comply with government regulations and business laws such as the Prevention of Transfer of Criminal Proceeds Act. In 2023 it raised JPY 1.5bn (GBP 7.53m) from backers such as JIC Venture Growth Investments (the VC arm of the Japanese Government), SMBC Venture Capital, Mizuho Capital, and the Sony Innovation Fund. Trustdock has been the most installed eKYC app for the past three years running and won the Emerging Partner of the Year award for AppExchange Partners at the Salesforce Japan Partner Awards 2024.

Spider Labs

Spider Labs is a startup specialising in anti-ad-fraud through its main product Spider AF. Spider AF can be used to detect click bots, scammers, and spam that attempt to increase ad running costs through artificially inflating traffic. It also protects companies' brand image through preventing the running of advertisements on gang affiliated or adult entertainment sites. It raised JPY 550m (GBP 2.76m) in Series B in 2021 receiving funding from Headline Asia and Mitsubishi UFJ Capital. Spider AF has already been implemented by large Japanese corporates such as Monex, SBI Securities Group, Shiseido, and JAL.

Opportunity areas for UK companies

Japan lags in the deployment of cybersecurity measures across all sectors. This fact can be seen as a challenge and as an opportunity. Introducing new cybersecurity technologies to the Japanese market requires patience and extensive education of the market.

IT and telecommunications

IT and telecommunications is the most established sector in terms of focus of cybersecurity measures, but Japan is behind in the implementation of cybersecurity solutions, especially given the rapidly increasing complexity of attacks. According to the Anti-Phishing Council, the number of reported phishing incidents in 2023 exceeded one million, an increase of 20 times compared to 2019. Amidst increasing pressure from the government and regulatory advisories, the endpoint security market is expected to grow along with the ID management market.

Cybersecurity continues to be the focus of IT investment by Japanese companies. Approximately 70 percent of Japanese companies use cloud, and the number is expected to grow. On average a company has over 50 security tools in place, it is expected that there will be increased investment opportunities for comprehensive and cross-functional products for cloud security.

UK companies offering the following technologies are encouraged to explore opportunities in Japan:

- **Automated, AI-integrated cybersecurity tools** to increase response time and reduce workload
- **Simplified multi-factor authentication** (the implementation rate of multi-factor authentication is about 90 percent overseas, but only about half in Japan)
- **Secure backup** measures for remote storage and restore tests
- **Comprehensive and cross-functional cloud security** products integrated onto one platform
- **Hybrid data centres** that allow companies to keep sensitive data on premise whilst allowing non-sensitive data to be retrieved through cloud to be accessed anywhere
- **Robust antivirus** software and real-time threat detection systems
- A system that unifies security logs, events, and responses under a single management platform to help manage a company's cybersecurity landscape effectively across multiple locations with smaller teams

Manufacturing

Traditionally Japanese companies have had a false sense of security as factories were operated as closed network environments. However, due to increased usage of cloud, IoT, AI and automation, as well as the convergence of information technology (IT) and operational technology (OT) systems that creates new vulnerabilities in the OT network via the IT network, Japanese companies are becoming increasingly aware of the need to address cybersecurity threats in the manufacturing sector. Reports of Japanese manufacturers and operators of critical infrastructure halting operations due to a cyberattack are bringing an increased sense of urgency. Examples include Toyota shutting down 14 factories in Japan in March 2022 and lens manufacturer Hoya stopping production in April 2024 because of a suspected breach.

Despite rising concerns, Japanese manufacturers have been slow to take concrete measures. The main challenge has been that IT teams that are now required to look after OT cybersecurity did not possess sufficient knowledge of the needs specific to production environments. Further, factory staff lack IT and cybersecurity knowledge. Bridging this gap remains a challenge.

Lack of regulation is another factor contributing to slow deployment of OT cybersecurity measures. The government is increasing efforts to accelerate the deployment of cybersecurity measures by the manufacturing sector, but currently there are no mandatory requirements, only guidelines. In November 2022 METI published "The Physical/ Cyber Guidelines for Factory Systems" that outlines vulnerabilities and demonstrates approaches to secure factory environments. "Key Considerations for Promoting Smartification" was issued by METI in April 2024 to further raise awareness among Japanese corporates engaged in smart factory initiatives. METI also allocates an annual budget of several billion yen, of which approximately JPY 30bn (GBP 0.15bn) is allocated to research and development and JPY 200bn (GBP 1bn) is designated to support security measures for small and medium-sized enterprises.

Recently the situation has been rapidly changing, with OT cybersecurity increasingly becoming a focus for many solutions providers including Fujitsu, NEC, Macnica and IIM (part of Seiko Group). Vendors of industrial control systems have been actively engaging in this space as well. For example, Yokogawa Electric launched an IT/OT security operations center in August 2022 and Mitsubishi Electric announced partnerships with Nozomi Networks, Dispel and TXOne Networks to enhance its one-stop OT security solutions offering in February-March 2024. This creates opportunities for UK companies offering OT cybersecurity solutions to explore interest with Japanese manufacturers.

Operational Technology systems are becoming a focus for security providers due to increased usage of cloud, IoT, AI and automation within critical infrastructure and manufacturing sectors.

Automotive

Connected cars, autonomous vehicles, AI-enabled smart cockpits and ADAS are key technology areas. Many Japanese OEMs are moving towards software designed vehicles (SDVs), integrating new technologies such as payment systems for connected cars. More of these connected cars are expected to be on the road as Japan's Cabinet Office has implemented the "Autonomous Driving Strategy Headquarters," aiming to put level 4 autonomous vehicles into practical use by 2025. Japan Automobile Manufacturers Association (JAMA) highlighted in its cybersecurity guidelines 2.0 (released in 2022) that the automotive industry is entering a period of technological change which increases cybersecurity risks.

The Japanese automotive sector is investing more in cybersecurity. Toyota is collaborating with Trend Micro to develop threat detection solutions and invested in Security Operation Centers (SOCs) for real-time monitoring. Nissan has partnered with NTT Communications to secure connected vehicle systems, while Honda has been working with McAfee on cybersecurity protocols.

Toyota, Nissan and Honda are adopting secure development practices and participating in industry alliances like Auto-ISAC and are leveraging AI for advanced threat detection and educating consumers on securing connected features.

Japanese automotive manufacturers need to align themselves with international regulations as a large proportion of their market is abroad. For example, ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering) and UN regulations on cybersecurity (UN-R155 CSMS) are required for new models with OTA updates from July 2022 in Japan, and for all models already sold from July 2024. It is further evident that the automotive sector is taking cybersecurity development seriously as guidelines have been developed by the Japan Automobile Manufacturers Association (JAMA) and Japan Auto Parts Industries Association (JAPIA) to enhance measures throughout the entire automobile industry. Also, 116 Japanese companies, including Toyota Motor and Hitachi, are collaborating to establish comprehensive industry standards related to software bills of materials (SBOMs) for automotive cybersecurity.

Opportunities for UK companies in the automotive cybersecurity space include:

- **Solutions to secure communication protocols** for V2X
- Services ensuring the **security of over-the-Air (OTA) updates**
- **Automotive intrusion detection systems** (IDS)
- **AI-driven threat detection** systems
- Protection against evolving **quantum threats**
- Solutions to streamline/ensure **compliance with international cybersecurity regulations** such as UN-R155
- **Solutions to detect vulnerabilities** and allow vendors to quickly assess if a cyber-threat has impacted its cars - currently there is no such system for the automotive industry in Japan

Healthcare

With an increased adoption of digital technologies, such as telemedicine and IoT medical devices, Japan's healthcare sector has become more vulnerable to cyber-attacks. The diversification of sophisticated cyber-attacks has created a need for proper management and operation of medical information systems, including electronic medical records. As an example, Keio University is creating a "smart hospital" funded by the government, which leverages IoT solutions to monitor patients. In the future, we expect to see more robotics for care connected to cloud and opening the market for cybersecurity in device management.

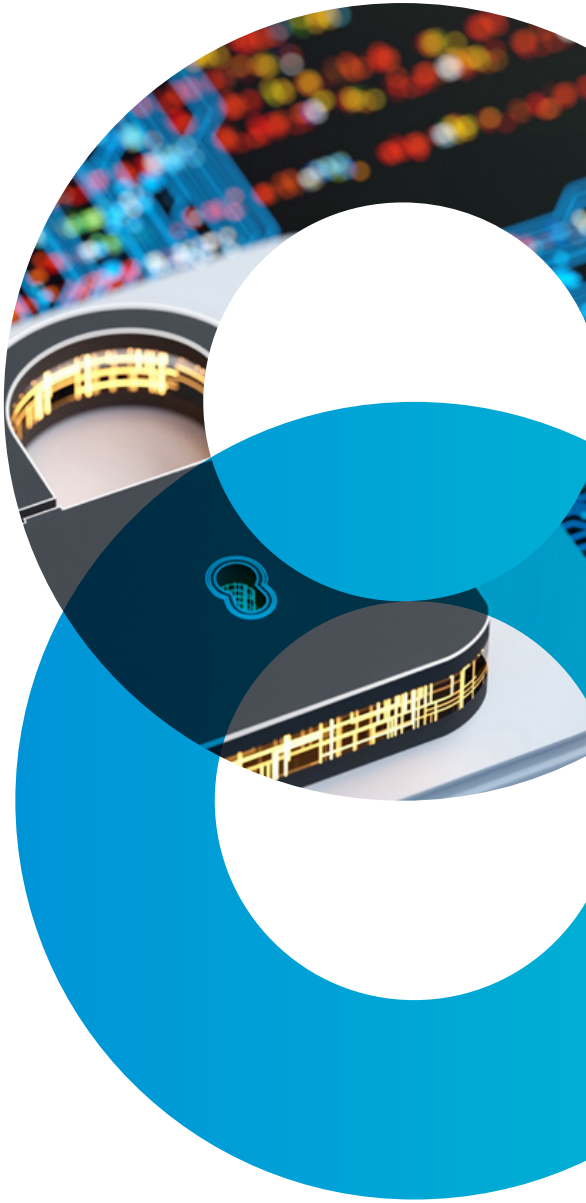
In 2021, METI and MIC introduced "three ministries, two guidelines" to better protect personal information, ensure safe handling of medical information data and to protect healthcare systems from cyber-attacks. These guidelines further recommend that institutions obtain ISMS certification to manage information security. Implementation of these guidelines for healthcare institutions is essential as less than 30 percent of Japan's hospitals are ready for cybersecurity attacks.

In March 2023, Japan outlined a new medical device cybersecurity regulation to ensure safety and basic performance. Medical devices using software are now required to implement risk management throughout the medical device software life cycle and medical devices connected to the internet must reduce the risk to acceptable levels.

In the healthcare sector, Japan lacks sufficient data encryption and incident response protocols, and still heavily relies on at-risk legacy systems, and therefore there are opportunities for UK companies with the following technologies to explore interest in the Japanese market:

- **Advanced threat detection and response systems** to identify and mitigate cyber threats in real-time
- **Data encryption** to prevent data from being lost or stolen
- **Secure communication protocols** to protect sensitive patient data and ensure privacy compliance with APPI
- **Firewall** solutions for hospitals using intranet systems
- **On premise data management** that can flag unauthorised access and have a kill switch for the hard drive in case date is stolen or lost
- **Advanced access management solutions**

It may be difficult for a foreign company to directly target the healthcare sector as Japanese hospitals/ healthcare centres do not want patient data to leave the country and therefore prefer to work/partner with Japanese companies. Therefore, foreign companies targeting Japanese healthcare market are advised to explore a channel strategy to enter the market.



Government and defence

Japan's government and defence sector is increasingly targeted by sophisticated cyber-attacks that threaten critical infrastructure, military systems, and sensitive government data. Recent incidents, such as state-sponsored attacks and cyber-espionage, have revealed vulnerabilities, including outdated systems, a lack of skilled cybersecurity professionals, and limited coordination among agencies. In 2022, the National Police Agency detected approximately 7,700 cases per day of suspicious access to Japanese entities, 2.8 times the amount in 2018 and almost all of which came from overseas. Japan recognises cybersecurity as a national priority and acknowledges the need to adopt more active defence measures to counter evolving threats.

The opportunities for UK companies in cybersecurity for government and defence are in:

- **Threat intelligence and automated response** systems for real-time detection and neutralisation of cyber threats
- **Implementation of AI and machine learning** that can enhance threat detection capabilities, automate response actions, and predict vulnerabilities to enable government entities to take a proactive approach to cybersecurity
- **Secure communication and data encryption** technologies critical to protect sensitive government and military information from unauthorised access and breaches

Due to regulatory restrictions in the government and defence sector, foreign companies cannot sell their solutions directly and need to work with local suppliers or defence contractors to engage this market.

Finance and banking

Japan's finance and banking sector faces increasing cybersecurity threats as digital transformation accelerates, exposing institutions to risks such as data breaches, ransomware attacks, and financial fraud. Recent cyber incidents involving major banks and financial institutions have revealed weaknesses, including outdated legacy systems, insufficient fraud detection mechanisms, and a lack of skilled cybersecurity professionals.

Financial institutions in Japan are increasing investment into cybersecurity focusing on securing online banking and payment processing systems, and protection of financial data and records.

For UK companies, key opportunities in the Japanese market are in:

- **Advanced fraud detection:** financial fraud prevention systems that use AI and machine learning can detect anomalies and prevent fraudulent transactions in real time that could also reduce the burden on human resources
- **AI solutions and automated defence** mechanisms that can detect and reduce third-party risks
- **Secure digital banking solutions:** including multi-factor authentication, end-to-end encryption, and biometric verification, are essential for protecting customer data and maintaining trust
- **Advanced security solutions for payments:** such as tokenisation, secure payment protocols, and fraud detection

Compliance with international cybersecurity standards such as ISO/IEC 27001 is crucial to ensure robust data protection and risk management

Success story:
Darktrace (UK)

Darktrace is a UK company offering cybersecurity solutions for threat detection. Darktrace uses AI algorithms to automatically detect and respond to cyber threats across physical, cloud, virtualised networks, IoT, and industrial control systems. As a self-configuring platform, it requires no setup and identifies advanced threats in real-time, including zero-days, insider threats, and stealthy attackers.

Darktrace established its Japan office in July 2015 and opened an office in Osaka in July 2019. In 2017 Darktrace signed a partnership with NEC Networks & System Integration Corporation (NESIC) to resell Darktrace's AI to NESIC's client base in Japan. Darktrace further signed J's Communication (2017) and Marubeni Network Solutions (March 2023) as partners in Japan.

Darktrace's customers in Japan include Otsuka Pharmaceutical, Keihan Holdings, and Netyear Group.

Routes to market

The Japanese market is perceived as difficult to enter, with its differences in culture, language and business practice. Further, Japanese companies are seen as slow-moving and bureaucratic. However, once relationships with Japanese companies are established, they tend to be long-lasting and robust. Japan values commitment and it is crucial to get market entry right the first time, as Japan is not usually forgiving to companies seeking to re-enter the market.

Japan-specific factors to consider:

- Speed – on average, sales cycles are 6 to 12 months longer
- Thorough technology validations – involve extensive Q&A including low-probability hypothetical scenarios to assess all possible risks and come up with response measures
- Specific applications – Japanese companies expect to be provided with specific applications and benefits of a new technology rather than exploring potential ways of leveraging it themselves
- Track record – Japanese companies do not like to be the first movers even if a solution is widely used overseas. Securing your first Japanese customer is crucial for success in the Japanese market
- Decision making process – consensus-based bottom-up decision-making that involves approvals from various stakeholders ('ringi'). Discussions at the top are useful to gain initial traction, but you will likely be referred to a technical team to carry out an evaluation after that
- Language – English is not widely used, but reading ability is higher than speaking. Technical support in Japanese in the local time zone is often essential

Market research

A company seeking to enter the Japanese market will require a strong understanding of industry needs specific to its product and the competitive landscape. Being proactive enhances the chance of successful entry and sustained growth. The UK-APAC Tech Growth Programme or information provided by Japanese government agency JETRO can be useful at this stage.

Exploring opportunities

The next step is to visit Japan and validate the opportunity through direct conversations with Japanese companies. Japan has become a lot more open to online meetings since COVID-19, but a physical visit and face-to-face conversations with the stakeholders are necessary to gauge real interest and start building relationships. A Japan visit can be done as part of a mission organised by the UK Embassy (as a stand-alone event or in conjunction with a trade show), an independent self-organised visit, or a visit planned by a partner. Other options could include joining open innovation programs of Japanese companies, partnering with an accelerator, or attending a conference.

It is increasingly possible to conduct initial meetings in English, but business decision makers can rarely converse in English. It is best to have a Japanese speaker on the team or hire an interpreter for key meetings. Localising materials is helpful but not mandatory.

Cybersecurity events in Japan

Event	Date	Website
Manufacturing Cyber Security Expo (Nagoya)	9-11 Apr 2025	www.manufacturing-world.jp/nagoya/en-gb/about/cybersecurity.html
IDC Cybersecurity Forum (Tokyo)	15-16 Apr 2025	www.idc.com/events/71945-idc-security-forum-2025-japan
Information Security Expo (Tokyo)	23-25 Apr 2025	www.japan-it.jp/spring/en-gb.html
AI in Cyber Security Summit (Tokyo)	02-03 Jun 2025	cognitivetechsummit.com/ai-cyber-security-conference/
Manufacturing Cyber Security Expo (Tokyo)	9-11 July 2025	www.manufacturing-world.jp/tokyo/en-gb/about/cybersecurity.html
Information Security Expo (Osaka)	21-23 Jan 2026	www.japan-it.jp/osaka/en-gb.html

Market entry strategies

A UK company can initially explore opportunities in Japan from overseas, but it is recommended to have a local presence to effectively drive discussions with Japanese companies and show commitment to the market. Establishing a Japanese entity may have tax implications and is time consuming. It is more common to start by appointing a local agent or a partner and making regular visits to Japan.

Distributor

Distributors provide access to a wide customer network; help manage relationships and offer technical support. A company seeking to enter the market will need to invest time to identify and train the right partner.

It is important to validate that your potential partner's existing customer base includes your priority target customers, as Japanese distributors tend to focus on inside sales and are reluctant to use a cold approach. Ideally, your potential partner should also have experience selling similar products (hardware vs software vs services), as Japanese companies struggle to apply their sales skills to a new offering type.

If your product is hardware, trading companies can be a good potential partner as they possess language capabilities, a wide customer network, and experience with import procedures. However, they usually have low technical capabilities, so it may not be the best option for complex solutions. Trading companies can provide first-level support but are unlikely to drive pilots or commercial deployments.

System integrators are an important type of partner to consider. Many Japanese corporates don't have extensive in-house IT capabilities, turning to system integrators for consultations and deployment of new solutions. System integrators are a great partner if your product can augment their solution/service offering, but they may not be the best primary distribution/reseller partner, since they are driven by customer needs and may work with multiple vendors. Nevertheless, having a large system integrator as a partner is extremely beneficial for customer discussions and raising your profile in Japan.

Augmenting your channel strategy by engaging a sales agent or hiring an initial direct employee can be transformative in increasing the effectiveness of distribution partners.

Joint venture

A joint venture can be an efficient market entry strategy, but it will take time to select the right partner, determine the structure of the joint venture and negotiate the terms.

Licencing

Direct licencing and franchising can be the most straightforward market entry strategy as it can be accomplished without a local partner or establishing a Japanese entity. However, a UK company will often require Japanese-speaking staff (or a bilingual person in Japan) and in-country technical resource to facilitate the conversations with potential partners.

Agent

Appointing a local sales agent – an individual or an organisation - to carry out business development activities and negotiations on your behalf will provide an advantage of having in-country support and a way to effectively manage relationships and business discussions with Japanese companies. This strategy allows you to augment or replace them by hiring local staff. This strategy is particularly suitable for companies with complex solutions that require extensive communication with the overseas teams.

Investor

Seeking investment from a Japanese VC or corporate and leveraging its connections to secure initial deals is another strategy a company seeking to enter the Japanese market could explore.

Setting up local entity

Japanese companies value a local presence, so it is recommended to establish an entity in Japan once initial business and relationships have been established. The main types of entity a foreign company can choose from are a representative office and a subsidiary.

Representative office

A representative office is the most basic form of in-country representation and a good option for the initial stage of market entry. Representative office can engage in market research, information gathering, purchasing, and advertising, but cannot perform sales activities. No formal registration is required but support from the main office or the local representative may be needed to open bank accounts or rent property.

Subsidiary

Japanese employees prefer to be hired by a Japanese entity; therefore, it is recommended to set one up when hiring local staff. A foreign company will typically choose between a joint-stock corporation (Kabushiki-Kaisha (K.K.)) or a limited liability company (Godo-Kaisha (G.K)). There are service providers that assist with the registration – the process usually takes six to eight weeks and costs GBP 7,000 - 8,000.

Establishing a Japanese entity can have tax implications and is time consuming, but is well valued by potential customers Achieve initial business through a local agent or partner, make regular visits to Japan, and then look to set up a local presence.

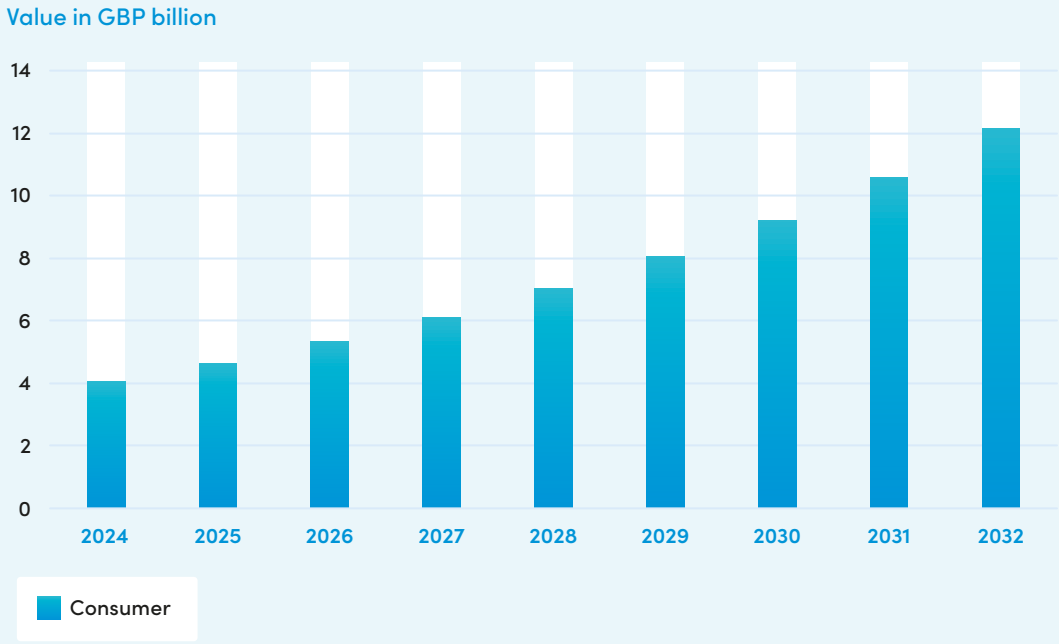
South Korea's cybersecurity market

Market overview

Size of the market

South Korea's cybersecurity market is estimated to be worth GBP 4.06bn in 2024. The industry is projected to develop at a compound annual growth rate (CAGR) of 14.70% between 2024 and 2032 to reach nearly GBP 12.15 bn by 2032. As one of the most advanced markets globally in terms of digitalisation, Korea continues to build out its digital environment across both the private and public sectors. However, due to this high level of connectivity, the country inevitably faces an ever-increasing number of cyber threats.

South Korea's cybersecurity market – expected growth



Source: Statista / Intralink research

Market trends

- **From cloud migration to cloud security –** Cloud security solutions have shown strongest growth rates over the last couple of years across the private and public sectors as both sets of organisations have been migrating their operations to the cloud, particularly after the COVID-19 pandemic. The pandemic pushed Korean enterprises and governments to accelerate the digital transformation and to make more everyday activities possible to achieve remotely. While cloud migration increases, it has opened up a new market for the cloud Managed Services Providers (MSPs), and as a consequence, for Managed Security Service Providers (MSSPs).
- **The Zero Trust Roadmap –** In light of the rapid growth of AI, machine learning, blockchain, and the Zero Trust initiative (a programme outlined by the Ministry of Science and ICT in 2023 to mandate identify verification for every user or device trying to access resources on a network), Korean cybersecurity firms have been trying to meet domestic security demands by actively adopting new technologies. AhnLab and ESTSecurity, who specialise in security control services and anti-virus solutions, have developed AI-based detection models to predict and mitigate cyber threats. In 2024, four consortia of domestic companies have been set up to work on government pilot projects related to this area.
- **Security solutions for the AI era –** As more and more companies and organisations use generative AI tools such as OpenAI's ChatGPT and Google's Gemini across their operations, there is a need for protection against unintentional data leakage in the process. Accordingly, a security layer or platform that allows enterprise customers to run AI and be data compliant is in increasing demand. For instance, Fasoo, a Korean cybersecurity company focusing on data security, has launched security solutions that prevent information leaks.
- **Going abroad –** It is worth noting that Korean information and cybersecurity companies are increasingly looking to expand overseas despite a decrease in export in 2023 that was approximately GBP 937m comparing to the export of GBP 1.11bn in 2022. The government has outlined a few initiatives to boost the growth of domestic companies with the regional focus on the Middle East and Southeast Asia, where Korean companies will be exposed to a broader network of international partners and customers. In addition, the government has also established K-Security alliance and cluster belts to allow domestic players to collaborate, as well as to advance its technical capabilities to compete on the global stage.

Challenges

Attacks on SMEs

According to the Ministry of Science and ICT (MIST) and the Korea Internet & Security Agency (KISA), along with Cyber Threats Intelligence Network, there is an increasing number of cyber hacking and ransomware attacks with 620 attacks recorded in 2020 jumping to more than 1,200 attacks in 2023. Most of the multi-extortion ransomware attacks are aimed at Small and Medium Enterprises (SMEs), representing a serious danger to the Korean economy and the manufacturing sector specifically, as SMEs are account for 39.3% of national exports and 81% of the country's employment rate. Korean SMEs are more vulnerable to cyber threats as they invest comparably less budget in information security. In November 2023, SMEs reported the highest rate of ransomware attack at 78.1%, compared to large corporations at 2.1% and mid-sized corporates at 14.8%.

Attacks on civilians

According to the Organization for Economic Co-operation and Development (OCED), Korea boasts the world's best digital accessibility across several parameters, ranked first in terms of the percentage of households with access to the broadband internet at home (99.96%), mobile internet (99.98%), and high-speed internet penetration (87.31%). In their daily lives, Korean citizens can effortlessly use internet services in the consumer, financial, administrative, medical, and other sectors thanks to this advanced infrastructure.

The hyperconnectivity across society, however, makes individuals vulnerable to cyber and phishing attacks targeting their personal information.

In February 2023, LG Uplus, one of Korea's three main telecommunication companies, experienced a major data leak where 300,000 of its users' information were exposed on the dark web. It turned out that the attack targeted the Customer Assistance System (CAS) for user services (authentication, subscription, and cancellation). In January 2023, Interpark, one of the largest ticket booking platforms, was attacked by credential stuffing, a method that randomly inputs user account data collected from other sites and attempts to log in, which resulted in the data of nearly 800,000 users being exposed. Phishing attacks toward unspecified civilians are continuously reported. In 2023, there were approximately 370,000 cases of smishing texts that attempt to install malicious files by inducing clicks on URLs within text messages, pretending to be a delivery service, a traffic fine or a family message.

Geopolitical hurdles

South Korea has faced an unsettled geopolitical landscape for decades and North Korea has been one of the major sources of those threats. In March 2023, MagicLine, an authentication security software that must be installed when accessing government services in Korea, such as the National Tax Service (year-end tax settlement), Korea Customs Service, or financial transactions, was confirmed to have been hacked.

In June that year, the incident was escalated to the National Intelligence Service, as not only was it confirmed that Lazarus, a North Korean hacker group, was behind it, but also the group had caused collateral damage by hacking more than 50 companies that had installed the software.

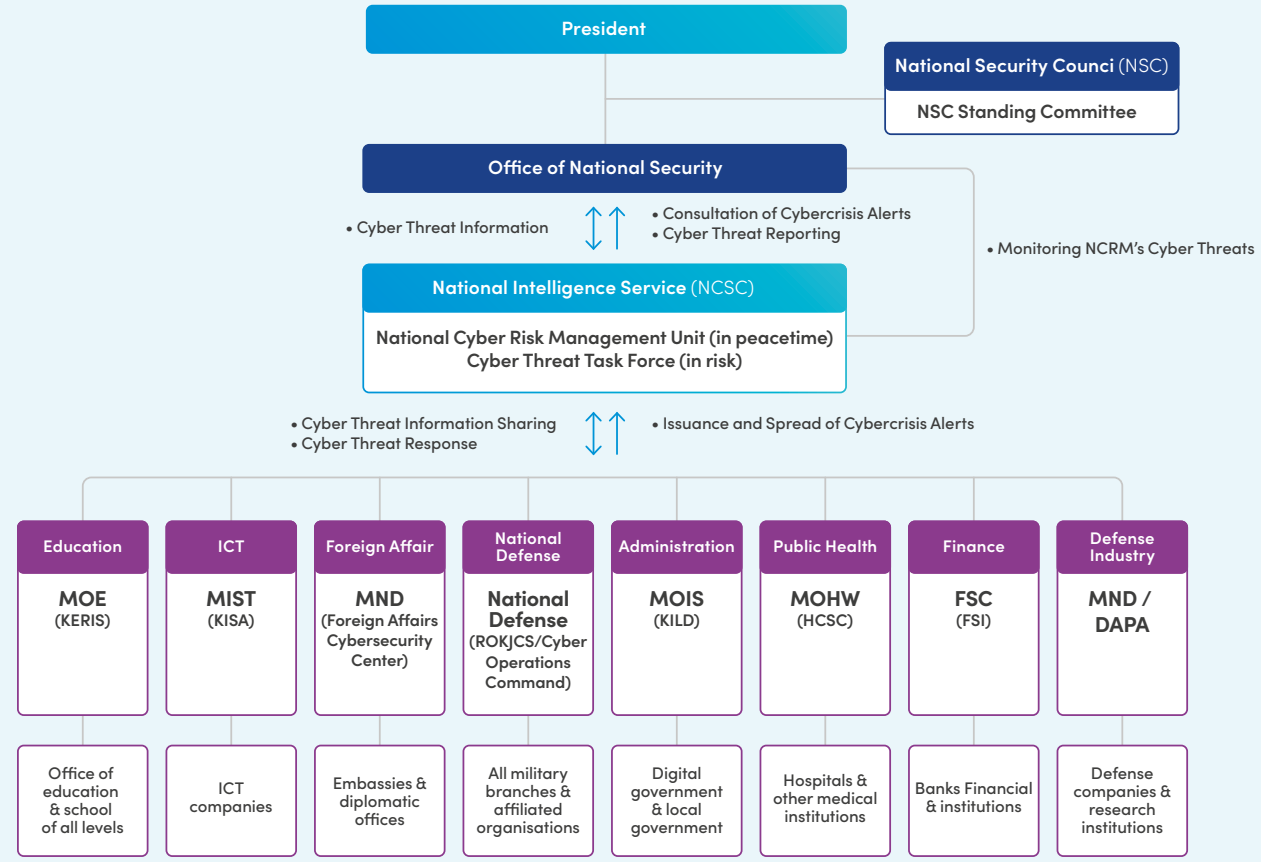
In August 2024, the intelligence authorities reported that North Korean hacking cells are particularly active in attacking SMEs in the defence, aviation, satellites, and shipping areas to obtain classified information, taking advantage of the companies' weak security. As the North Korean hackers have expanded their activities across borders to steal nuclear and military secrets, the South Korean government has recently issued a joint warning with the UK and US authorities to find the ways to strengthen its national security in this area.

Public sector initiatives

The South Korean government has designated the Office of National Security (ONS) as a control tower for managing overall national cybersecurity tasks; planning and reviewing mid to long-term policy schemes. Under the ONS management and supervision, National Intelligence Service (National Cyber Security Center) operates the practical duties against cyber risk and threat across the whole areas of the nation and the public. In alignment with the ONS, the NCSC responds to relevant ministries, expertise agencies, and companies with real-time threat information. The below table presents the main organisations and their roles and responsible regulatory framework. Each ministry carries out cybersecurity or information protection activities in its respective fields.

The Information Security Management System (ISMS) is the Korean version of the international ISO/IEC 27001 standard and provides a framework for organisations to manage their information in a secure manner. While it is not a mandatory regulation, the Korean government strongly urges organisations to adopt it, and it does mandate the system for Critical Information Infrastructure (CII) operators in sectors like energy, finance, telecommunications, water, and transportation, and public institutions, among others.

South Korea's national cybersecurity implementation framework



Source: 2024 National Cybersecurity White Paper

Public sector organisations

Name of organisation	Role
Office of National Security (ONS)	ONS assists the President's duties relating to national security and deliberates national security policy. Its latest publication in February 2024, National Cybersecurity Strategy, provides the top-level guidance in cybersecurity in the context of national strategic direction
National Intelligence Service (NCSC)	NCSC is the central operational agency to: ○ collect, comply, and distribute cybersecurity intel in all areas of the country that include international and state-sponsored hacking organisations ○ confirm, deter, and block security violations by North Korea and other foreign countries ○ carry out countermeasures for national security
Ministry of Science and ICT (MSIT)	MSIT oversees and settles private sector cyber and information security policies and frameworks. It establishes and operates systems to prevent and respond to private sector intrusions, designates key information infrastructure facilities, analyses and evaluates their vulnerabilities, and oversees electronic authentication. MSTI's Critical Information Infrastructure Protection Act protects national key industries and guides organisations to keep themselves from cyber-harm.
Ministry of the Interior and Safety (MOIS)	MOIS enhances cybersecurity breach response in digital governance through the 17 Cyber Attack Response Centers it operates jointly with the National Information Resources Service, Korea Local Information Research and Development Institute, and metropolitan governments.
Financial Services Commission (FSC)	FSC protects users who perform electronic financial transactions, and forms and improves information security policies and frameworks around electronic finance in accordance with acts, such as the Electronic Financial Transactions Act and Credit Information Use and Protection Act
Personal Information Protection Commission (PIPC)	The PIPC oversees and adjusts policies related to personal information as needed in today's data economy and cooperates with relevant entities in preventing and responding to personal information breaches
Korea Internet and Security Agency (KISA)	KISA acts as a guarantor of the safety and reliability of information security through the certification of the Information Security Management System (ISMS), the Personal Information Management Systems, and cloud security.

Source: 2024 National Cybersecurity White Paper / Intralink research

Four strategies for securing global competitiveness

In September 2023, the Ministry of Science and ICT (MSIT) announced the 'Strategy to Secure Global Competitiveness in the Information Security Industry' to grow the domestic information security market to a value of GBP 17bn by 2027. Within that figure, it aims to grow the cybersecurity market to GBP 6bn, in part by enabling more domestic cybersecurity unicorns to develop. The government has allocated a budget of GBP 621mn to this initiative which aims to achieve four overarching aims:

- Zero Trust Transition Roadmap
  - Zero Trust refers to a cybersecurity model that is built on the concept of "Never Trust, Always Verify". Every access that is requested, whenever and wherever it occurs, requires verification. The concept contrasts with the conventional Perimeter Security Model. MSIT will be running pilot Zero Trust projects in the telecommunication, finance, medical, as well as other key sectors. As the security paradigm shifts to the Zero Trust approach, the government aims to build a new market for new security systems across the industries of the future such as smart factories, smart healthcare, robots, space, and aviation.
- Expanding a solid industrial ecosystem for global competitiveness
  - The government has appointed several regions for the K-Security Alliance & Cluster Belt: K-Security Cluster Belt across Pangyo for the security startup bed; Busan-Ulsan-Gyeongsang for strengthening regional security industry, and Songpa for a global security cluster
  - Under this strategy, the government also established a cybersecurity fund, aiming to invest a total of GBP 73mn by 2027, and aims to train up more information security professionals
- Securing next-generation information security technology competitiveness
  - The government is actively building relationship with leading countries in the cybersecurity, such as the United Kingdom, United States, Germany, and Finland, through a joint research, investment and acquisition of more advanced cybersecurity technologies
- Cooperating with emerging markets
  - The Korean government plans to build cooperation with emerging markets across the Middle East and Southeast Asia. The government sees both regions as strategically important markets to boost domestic companies' market expansion activities. This initiative also increases the possibility of winning large-scale overseas projects led by the public sector through the formation and support of a public-private cooperation in the Middle East and Southeast Asia, enhancing the indirect export effects for domestic companies through their participation in such projects

2024 National Cybersecurity Strategy

The National Cybersecurity Strategy was revealed in February 2024 by The National Security Office, outlining 5 major strategic tasks, each aimed at advancing national security capabilities through a coalition of government, industry and academia. Those tasks are:

- A defensive-to-offensive response shift towards the cyberattacks from North Korea
- A stronger infrastructure resilience with a classification system to identify and rank cyber attacks
- A cyber risk management system with a focus on emerging technologies, such as AI and quantum
- A public-private data sharing platform to unify the national response to cyberattacks
- Global cooperation with leading cybersecurity countries to exchange best practices and train workforce

UK-Korea Strategic Cyber Partnership

In November 2023, the three key cooperation tasks of the cyber partnership were selected between the UK and Korea under the Strategic Cyber Partnership. Specifically, the two countries agreed to strengthen the foundation of the information security industry and personnel through providing access to various security markets, collaboration in research and development of core technologies, joint training, and personnel exchange. Under the partnership, there are a number of government programmes and initiatives that seek to fund collaboration between the companies and organisations from both countries.

Key players

Domestic leaders

Korea's domestic cybersecurity industry is led by the so-called 'Big 3' – SK Shielders, Ahnlab, and Secui – who supply their solutions and services into domestic conglomerates, financial institutes, and government agencies. Ahnlab, established in 1995, provides integrated security platforms that protect and respond to multiple security areas, such as endpoints, networks, clouds, services, security operations (SecOps), and operational technology (OT). It offers its products across both - private and public sectors, including financial institutions. SECUI, a subsidiary of Samsung SDS, provides network security, cloud security and threat analysis. SK Infosec, a subsidiary of the SK Group, and ADT Caps merged in November 2020 to form SK Shielders.

Cybersecurity ecosystem

Regulators

- Ministry of Science and ICT
- Ministry of the Interior and Safety

Key players

AhnLab, SK shieldus, WINS, IGLOO, ESTsecurity, SECUI

Next generation cybersecurity

DREAM SECURITY, NORMA, EYLIB

Government agencies

KISA

Start ups

CRYPTO LAB, SECURITY PLATFORM, Tatum Security, AI Spera, DEEPING SOURCE

System integrators

SAMSUNG SDS, SK 주식회사 C&C, MEGAZONE CLOUD, BESPIN GLOBAL, LG CNS

The rapid demand and growth in recent years has ensured that the key players are keen to engage with external innovation sources to keep up with cyber tech developments. AhnLab, for example, has aggressively expanded its presence through a number of acquisitions acquiring a cloud company CloudMate, AI security startup Jason, and OT security solution company Naonworks.

The company has also made small investments and partnered with domestic startups, such as Spiceware, Waikikisoft, Datum, Astron Security, Monitor Lab, and Pescaro.

Key players in the cybersecurity industry

Name of organisation	Website	2023 revenue (GBP)	Employees	Key products
SK Shieldus	www.skshieldus.com	1.03bn	6,500	Industrial and enterprise network and system security products and maintenance services, AI CCTV and OT solutions
Ahnlab	www.ahnlab.com	135m	1,320	Antivirus, online security, network security, firewalls, IPS and UTM
SECUI	www.secui.com	81m	480	Intrusion prevention systems, anti-DDoS security, vulnerability analysis, unified management systems
IGLOO Corporation	www.igloo.co.kr	60.4m	1,020	Managed security service and enterprise security management
WINS	www.wins21.co.kr	60.3m	488	Intrusion prevention, firewall, DDoS response, APT protection, integrated security monitoring, video privacy
ESTsecurity	www.estsecurity.com	14m	193	Endpoint security, corporate asset protection, APT attack response, ransomware response, threat detection and analysis

Source: Intralink research

Emerging startups

Innovation in cybersecurity is also being aided by Korea's thriving start-up environment, as many growing businesses are creating innovative solutions in the fields of quantum, blockchain, and AI. Crypto Lab, a company specialising in encryption technology, provides data protection solutions using homomorphic encryption and quantum encryption. It develops technology to safely handle sensitive data in the financial and healthcare fields. Crypto Lab was selected as a standard company that commercialise homomorphic encryption, beating major global IT companies such as MS and IBM.

Another startup Deeping Source uses AI and deep learning technology to provide a solution for de-identifying video data. Its technology covers up personal information in videos captured on CCTV and collects only the data that differentiates itself from competitors and resolves legal and moral issues. Security Platform has developed an IoT security technology for semiconductors to protect users' personal information. It has partnered up and secured investment from Softbank, the parent of ARM, for creating synergies with ARM's next-generation IoT processor.

Sandslab, specialising in AI security, has partnered up with LG Uplus and KAIST to jointly develop cybersecurity-focused sLLM (smaller Large Language Model) and a pilot platform. The consortium secured a fund of GBP 5.6mn from the Ministry of Science and ICT (MIST) and the Institute for Information and Communications Planning and Evaluation (IITP) for the 'Information Protection Core Source Technology Development Project' to be executed from 2024 to 2027.

Key startups in the cybersecurity industry

Name of organisation	Website	2023 revenue (GBP)	Employees
Crypto Lab	www.cryptolab.co.kr	0.2m	58
Deeping Source	www.deepingsource.io	1.2m	46
Security Platform	www.securityplatform.co.kr	2.8m	30
AI Spera	www.aispera.com	2.2m	49
Tatum Security	www.tatumsecurity.com	0.4m	29

Source: Intralink research

Opportunity areas for UK companies

Automotive

Korea's automotive industry is facing increased demands for cybersecurity solutions, as its top automaker Hyundai Motor Group and the government have focused on making the country more competitive in the global market for connected cars and autonomous vehicles. In September 2022, Hyundai Motor Company announced an investment of GBP 10bn over the next several years to shift all of its car models to Software Defined Vehicles (SDVs) that are applying wireless software updates, so-called Over-the-Air (OTA) software updates, which allows all vehicles sold around the globe from 2025 to have performance and features updated even after being purchased. At the same time, the Ministry of Land, Infrastructure, and Transport has planned to commercialise fully autonomous vehicles (Level 4) that do not require driver intervention by 2027 and to increase the penetration rate of new vehicles with autonomous driving functions to more than 50% by 2035.

The country's major shift to connected and self-driving vehicles, however, brings increasing exposure to cyber threats as the vehicles are increasingly connected to communication networks and this means that the leading automakers are internalising cybersecurity capabilities.

For instance, Hyundai AutoEver, Hyundai Motor Group's subsidiary developing automotive software, offers an in-house security solution, Mobilgene Security, and has developed firewall and Intrusion Detection System (IDS) technology for vehicle Over-to-Air (OTA) security. In August 2022, the group also acquired Cyber Security Management System (CSMS) certification based on ISO 21434, an international standard for cybersecurity engineering, through 42dot, the group's subsidiary that develops automotive software and mobility platforms.

As car parts become increasingly electrified, and these electrical parts and services are connected through software, external access channels to operating software registered in the vehicle have increased, which can increase their vulnerability. HL Mando, a global tier-1 OEM that specialises in electric vehicle and autonomous driving solutions, has partnered with Argus Cyber Security, an Israeli firm specializing in automotive cybersecurity solutions, to apply Argus' solutions to its electric vehicle system products since 2022. In 2021 LG Electronics expanded its business portfolio to the automotive electronic equipment and component solutions, acquiring 64% of Cybellum's shares, an Israeli cybersecurity company, to advance its level of cybersecurity. Early in 2024 this strategic acquisition resulted in launching the Cyber Security Management System (CSMS) platform for monitoring and maintaining vehicles' cybersecurity.

The UK's expertise in automotive cybersecurity solutions can help Korea to enhance the quality of its automotive security measures in:

- **Software Defined Vehicles (SDV):** It is worth noting a recent commercial development partnership between four Korean and British companies to design security solutions for Software Defined Vehicles (SDV) environments: Autocrypt, a Korean autonomous driving security company; Korea Automotive Technology Institute (KATECH); Beam Connectivity, a British connected car company; and Secure Elements, a British mobility security company.
- **Over-the-Air (OTA) software & Intrusion Detection System (IDS):** One of the key technologies Korea aims to develop and deploy is a real-time security monitoring system using Over-the-Air (OTA) software updates and the Intrusion Detection System (IDS) to the automatic transmission electronic control unit (TCU) from 2023 to 2026.

Manufacturing

Korea is a global manufacturing powerhouse with strengths in industries ranging from electronics, automobiles, semiconductors to fast-moving consumer goods. Korea's manufacturing sector accounts for 27.5 % of its total GDP, which is high compared to other major OECD countries, and Korea ranks third out of 152 countries, following Germany and China, in the Global Manufacturing Competitiveness Index published by the United Nations Industrial Development Organization (UNIDO).

In recent years, interest in cybersecurity has increased due to the growth of industrial automation that combines Operational Technology (OT) and Industrial Control Systems (ICS), along with IoT and smart factory solutions. Conventional OT networks have operated as closed networks, making it impossible to penetrate from the outside. However, a rapid digital transformation in the manufacturing sector has seen production lines and facilities change into so-called smart factories often connecting to external networks, new IoTs and cloud environments, exposing OT networks to potential cyberattacks. According to a recent survey, while 79% of domestic manufacturing companies are operating more than 100 OT devices with internet communication functions, 8 out of 10 OT managers experienced at least one intrusion in the past 12 months in malware attacks (44%), phishing emails (35%), and Distributed Denial of Service attacks (DDoS 33%).

Korean companies are increasing their investment in and collaboration activities with foreign OT security solutions. Claroty, an Israeli startup that protects all cyber-physical systems (CPS) across the Extended Internet of Things (XIoT), received GBP 7.7mn from LG Technology Ventures, a venture capital arm of LG Group, in 2021. This investment opened up a route to the Korean market, as the company signed a number of strategic partnerships with major corporate system integrators, such as LG CNS, Doosan Digital Innovation, and SK Shieldus.

British security companies have strengths in AI-based threat detection and response solutions, cloud security, and supply chain security, which should find a warm reception among Korean manufacturers. Therefore, UK cybersecurity firms in the following fields have many opportunities for collaboration with Korean players in manufacturing, IT, and cybersecurity:

- **ICS and OT security**
- **Smart factories**
- **Industrial IoT security**
- **Data protection**

IT and telecommunications

The Korean ICT infrastructure is amongst the most advanced in the world. However, as this infrastructure becomes ever more ubiquitous, so too do the cyberthreats. Recognising this, the large Korean telecommunications companies, KT, LG U+ and SK Telecom, as well as IT System Integrators (SIs), like LG CNS and Samsung SDS, are constantly introducing new security solutions in collaboration with overseas security experts.

- **AI-based security management technologies:** A notable case is Darktrace, the British cybersecurity company that specialises in machine learning and AI-based security solutions. In 2016, Samsung SDS, Samsung Group's subsidiary that provides IT solutions, invested in Darktrace to acquire cybersecurity capabilities for its ICT business and offer Darktrace's products in automated security threat detection, analysis, and blocking to the domestic market. In 2022, KT DS, KT Group's subsidiary that provides IT services, signed a partnership for distribution with Darktrace to expand KT's business coverage into AI-based security management technologies.

The Korean market offers a variety of market expansion opportunities for British cybersecurity companies as the country faces a shortcoming of cybersecurity experts despite a well-developed 5G network, AI, cloud, IoT, and quantum cryptography infrastructure, largely due to a lack of security experts domestically.

Healthcare

The Korean healthcare industry is rapidly becoming digitised and AI-driven, with medical IoT, cloud computing, big data and AI, telemedicine, and electronic medical records (EMR) being introduced. Korea's AI healthcare market was estimated to be GBP 290mn in 2023, growing 50.8 % a year on average, and is estimated to reach a market size of GBP 5.2bn by 2030. This steep growth is based on the country's 5G network infrastructure, a 90% electronic medical records (EMR) penetration rate, and an easy environment to obtain medical data as it is covered by a single national health insurance system. But as technology advances, there is also a greater chance of cyberattacks. In recent years, the importance of cybersecurity has increased as medical institutions have experienced hacking, ransomware attack, and data leaks of patients' sensitive information.

Korean hospitals are starting to adopt cloud and AI-based management systems to strengthen their security and monitoring infrastructure. Concerns around sensitive information leakage have been one of the biggest obstacles to developing AI models in the industry. However, in January 2024, Samsung Medical Center, one of the top domestic hospitals that leads digital medical innovation, built a customised AI model service environment using Microsoft's Azure Arc, a cloud management solution that blocks concerns about sensitive information leakage for the first time among domestic hospitals.

The Korea Health Information Service (KHIS) is also participating in the Global Digital Health Partnership Program (GDHP) to share its experience and cooperate with leading countries in the security technologies, including the UK.

As Korean healthcare organisations are increasingly adopting foreign technologies to meet international security standards, British companies stand a strong chance of succeeding in this area. UK cyber security companies can explore collaboration opportunities in the Korean healthcare sector in a variety of areas, including:

- **Intrusion detection systems (IDS)**
- **Threat monitoring**
- **Smart medical device IoT security**
- **Data security (encryption and pseudonymisation)**
- **Operating room CCTV security**
- **Cloud-based medical and hospital information system security**

Finance and banking

Seoul has recently been ranked first in future growth potential among 133 cities around the world according to the Global Financial Centers Index (GFCI) in 2024. It has also stepped up to 10th place globally in terms of financial competitiveness in fintech ranking and infrastructure. However, as digitalisation is rapidly progressing in the sector, cyberthreats targeting financial institutions are becoming more common and diverse. The importance of cybersecurity solutions is expected to grow significantly on the back of the Financial Services Commission's decision in August 2024 to partially dismantle the network separation regulation among financial institutions. The regulation has obliged domestic financial companies to manage external networks connected to the internet and internal networks containing personal financial information separately.

- **Cloud and AI solutions for financial transactions:** As the restriction is gradually being lifted, Korean financial businesses can now leverage AI services like ChatGPT to create new financial products. This opens up new avenues for them to adopt cloud and AI solutions from third parties, saving money by not having to develop everything from scratch and incurring large development costs.

British businesses have potential opportunities to work together or supply technology in fields including cloud security, financial data protection, and AI-based security solutions.

Homeland security and defence

Under the cooperative public and private bridge between the UK and Korea, UK cybersecurity companies could seize growing opportunities to collaborate with the Korean government and defence industry based on their advanced technologies and experience in the following sectors:

- **Supply chains encryption:** In November 2023, Korea's National Cyber Security Center (NCSC) of the National Intelligence Service (NIS) and the UK's National Cyber Security Center (NCSC) of the Government Communications Headquarters (GCHQ) announced their first cybersecurity joint advisory, the result of a cyber partnership signed between the two countries. The advisory observes North Korean state-linked cyber actors attacking supply chains through zero-day vulnerabilities and exploitable areas of third-party software. The bilateral cooperation between the two organisations is aimed at unpacking the techniques used by North Korean hacking cells on that country's recent supply chain software attacks and how to counter those tactics through technical collaboration with information security companies
- **Data protection:** Military secrets and important data protection are particularly critical within the geopolitical context of the Korean peninsula, being located adjacent to Russia, China, and North Korea with strong cyber capabilities, and the need for strengthened security is increasing as hacking and information leak incidents have increased in recent years. Accordingly, Korea is gradually expanding its investment in conducting joint research or introducing solutions with foreign authorities and companies
- **Cloud transition in space and defence:** In October 2023, LIG Nex1, a leading Korean aerospace and weapons manufacturer, signed a MoU for future space and defence cloud transition with Amazon Web Services (AWS) and Megazone Cloud, a Korean managed cloud service provider, to jointly plan research projects on the cloud computing in the defence and space sectors and cooperate with each other in technology exchanges. The agreement has enabled LIG Nex1 to prepare for the expanding space, cyber, and unmanned sectors while being supported in big data analysis, AI, and security power

Success story: Secure Elements (UK)

It is worth noting a recent commercial development partnership between four Korean and British companies to design security solutions for Software Defined Vehicles (SDV) environments: Autocrypt, a Korean autonomous driving security company; Korea Automotive Technology Institute (KATECH); Beam Connectivity, a British connected car company; and Secure Elements, a British mobility security company.

Secure Elements is a British cybersecurity company that provides automotive cybersecurity engineering software and AI-powered cybersecurity tooling solutions for mobility systems. It won the competition of the UK-South Korea bilateral commercial development jointly with the consortium members, granted by Innovate UK and Korea Institute for Advancement of Technology (KIAT). The collaborative initiative lays the groundwork for the applied cybersecurity technology of over-the-air software updates (OTA) and vehicle-to-everything communication (V2X), in which Korea's commercial demand has been presented.

Routes to market

Exploring opportunities

Comparing to western countries, Korea still has a strong preference for face-to-face conversations with the stakeholders to build a feasible interest and relationships. A visit to Korea can be done as part of a mission organised by the British Embassy (as a stand-alone event or in conjunction with a trade show), an independent self-organised visit, or a visit planned by a partner. It is increasingly possible to conduct initial meetings in English, but business decision makers can rarely converse in English. It is best to have a Korean speaker on the team or hire an interpreter for key meetings.

A UK company can initially explore opportunities in Korea from overseas, but it is recommended to have a local presence to effectively drive discussions with Korean companies, showing commitment to the market. Establishing a Korean entity may have tax implications and is time consuming. It is more common to start by appointing a local agent or a partner to secure an initial market presence, by also vising Korea regularly to advance relationships.

Direct sales vs channel partners

The Korean market is not without its challenges, particularly for companies seeking to do business in the public security sector.

UK companies may find the public sector procurement process difficult to navigate without an in-country partner, while regulatory differences may impede the adoption of new technologies. While it possible to sell direct from abroad to local companies, expectations on local language after sales support are very high in Korea.

When entering the Korean market, establishing a local channel partnership with a system integrator (SI) or value-added reseller (VAR) can become a great market reference that is so important to Korean customers. UK cybersecurity companies can benefit from a well-positioned partnership, especially in the public sector and in the procurement and regulatory processes that are so complex; and as the previous cases show, a well-managed partnership could also lead to a stronger commercial pipeline.

Agent

Appointing a local sales agent – an individual or an organisation - to carry out business development activities and negotiations on your behalf will provide an advantage of having in-country support and a way to effectively manage relationships and business discussions with Korean companies. This strategy is particularly suitable for companies with complex solutions that require extensive communication with the overseas teams.

Joint venture

A joint venture can be an efficient market entry strategy, but it will take time to select the right partner, determine the structure of the joint venture and negotiate the terms. It has the advantage of allowing a UK company to benefit from the partner's local knowledge and network while retaining more control that working through a channel partner.

Local investor

Seeking investment from a Korean VC or corporate and leveraging its connections to secure initial deals is another strategy a company seeking to enter the market could explore. Companies should not expect too much sales support from a local VC or CVC as they are often not set up to provide such sustained support for business development efforts.

Setting up a local entity

There are broadly three ways in which a foreign company can set up a presence in Korea. In order of level of financial and commitment and sophistication, these are a Liaison Office, a Branch Office and a Foreign Direct Investment Company.

Liaison office

A Liaison Office is recognised as a foreign corporation, but its core function is non-commercial, focusing on tasks such as market research and promotional activities for the parent company. It is a good option for foreign investors looking to establish a presence and assess the Korean market before formal business activities. Despite its limited scope, registration with the appropriate tax office is required.

Branch Office

A Branch Office operates as an extension of its foreign headquarters, legally considered one entity with the parent company. Branch offices can conduct profit-generating activities within Korea and are subject to the same tax laws and rates as domestic Korean companies.

Foreign Direct Investment (FDI) Company

Foreign companies can opt to establish a local FDI corporation. A minimum capital of KRW 100 million is required to be invested in the country. FDI companies may receive certain advantages under Korean law based on their specific activities.

Korea maintains a strong preference for face-to-face conversations to build relationships. Visiting the market regularly and using a local agent will help explore initial opportunities, but in-market partners will expect the eventual commitment of a local entity.

Trade shows and events

The largest international security conference in Korea is the International Security Conference (ISEC). It introduces security trends and issues and builds a platform for information exchange among 50 institutes and organisations. PASCON, which recently rebranded itself as Korea Cyber Security Conference (KCS CON 2025), is one of the largest cybersecurity conferences and security solutions exhibitions, with approximately 1,000 public, financial, and corporate information security officers and practitioners in attendance.

Cyber Summit Korea is hosted by the National Intelligence Service and the National Research Council of Science and Technology for domestic and international experts to discuss the latest technologies and policy direction. Last but not least, the Annual International Conference on Information Security and Cryptography (ICISC) is hosted by the National Security Research Institute and the Korean Institute of Information Security and Cryptology. This event invites research papers on all aspects of theory and applications of information security and cryptology.

Cybersecurity events in Korea

Event	Date	Website
ISEC, International Security Conference (Seoul)	26-27 Aug 2025	https://www.isecconference.org/2024/eng/
PASCON (Seoul)	8 Jul 2025	https://www.dailysecu.com/form/register.html?form_id=1701154152#a1
Cyber Summit Korea (Seoul)	10-12 Sep 2024	https://cybersummit.kr/eng
ICISC, The Annual International Conference on Information Security and Cryptography (Seoul)	20-22 Nov 2024	http://www.icisc.org/

Source: Intralink research

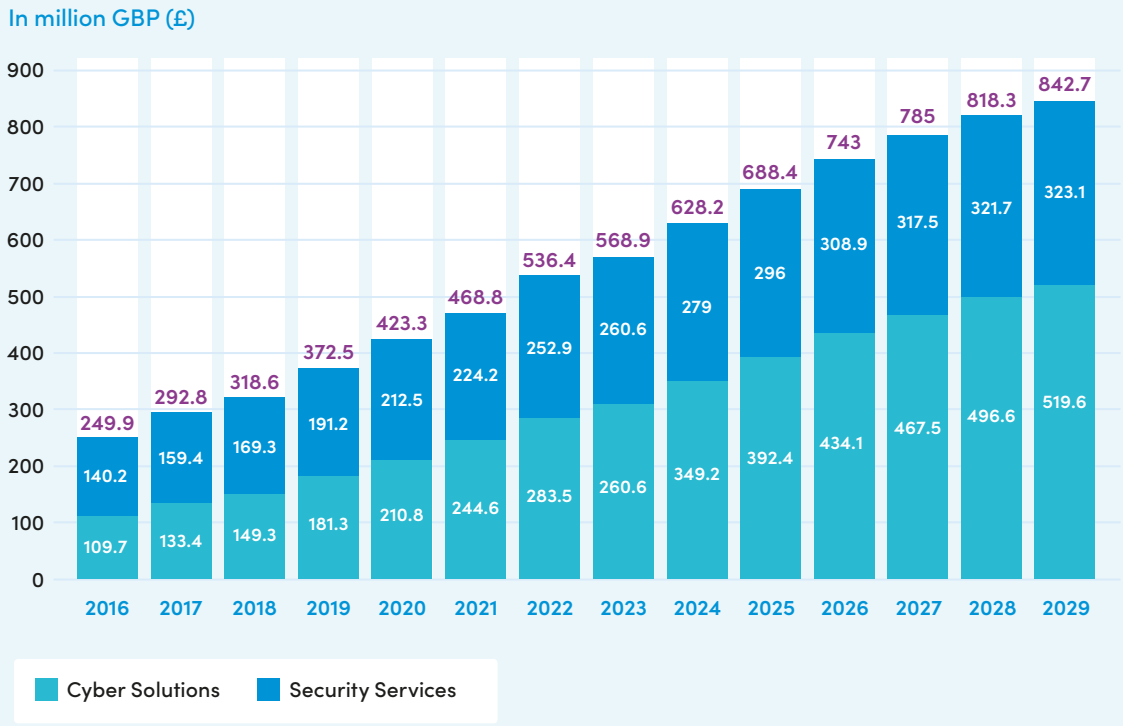
Taiwan's cybersecurity market

Market overview

Size of the market

Taiwan cybersecurity market revenue is projected to reach GBP 628m in 2024, with cybersecurity solutions accounting for a little over half with a projected market value of GBP 349m. The remaining value stems from security services. Total revenue is expected to show an annual growth rate (CAGR 2024-2029) of 8.27 percent, resulting in a market revenue of GBP 843m by 2029. The average Spend per Employee in the cybersecurity market is projected to reach USD 30.74 (GBP 23.11) in 2024. This is less than the global average of USD 52.16 (GBP 39.21).

Taiwan cybersecurity revenue by segment



Source: Statista Market Insights

Cybersecurity solutions are defined as products and services designed to meet an organisation's specific security needs, while security services are a broad range of services that enhance an organisation's security strategy against cybercrimes.

Cybersecurity solutions are automated technologies that help organisations monitor, detect, report, and counter cyberattacks. They include application security, cloud security, data security, and network security. They can also include firewalls, Distributed Denial of Service (DDoS) protection, micro segmentation, account takeover protection, Application Programming Interface (API) security, bot management, and web application security. Market revenue for Taiwan in cybersecurity solutions for 2024 will reach GBP 349m (56 percent of the overall cybersecurity market) and is projected to reach GBP 520m by 2029 (62 percent of the overall market).

Security services include design and integration, consulting, implementation, risk and threat assessment, and professional training and education. These services help organisations protect their networks and data from cyberattacks. Market revenue for Taiwan in security services for 2024 will reach GBP 279m (44 percent of the overall cybersecurity market) and is projected to reach GBP 323m by 2029 (38 percent of the overall market).

Market trends

Taiwan is a global leader in the semiconductor industry and a hub for technological innovation but increasingly finds itself vulnerable in the digital age. As the island embraces greater digital connectivity through 5G deployment and Internet of Things (IoT), robust cybersecurity measures are needed to protect its critical infrastructure, sensitive data, and ensuring the privacy of its 23.5 million citizens. The industry is growing and developing rapidly but it is also facing multiple challenges. The industry therefore demands innovative solutions from its cybersecurity startup scene, backed up by public sector initiatives and action.

Several trends can be discerned from Taiwan's cybersecurity landscape:

- **Escalating threats –** Latest data indicate a significant rise in cyberattacks targeting Taiwan. Google Cloud reported a 3,370 percent increase in DDoS attacks targeting Taiwan in the run up to its 2024 presidential election, compared to data from the previous year
- **High profile targets –** Such attacks often target critical infrastructure, public sector websites and digital assets, and high-profile private sector entities. There is also a recent trend in the rise of attacks against the financial sector and critical infrastructure such as power grids. In 2023, a major cyberattack disrupted the operations of Taiwan's state-owned electric utility Taipower, causing temporary power outages in several regions throughout the island
- **Economic impact –** The estimated cost of cyberattacks to the Taiwanese economy stands at over GBP 11.3bn annually, based on a 2022 study conducted by the Ministry of Economic Affairs (MOEA)
- **Challenging attribution –** Experts are unable to provide specific attribution to these attacks, but many point the finger towards Chinese-linked cyber actors launching sophisticated attacks to disrupt operations, steal sensitive information, and potentially sow civil discord. One such group typically cited is 'Blacktech', suspected of having ties to China and linked to multiple cyber-espionage campaigns targeting Taiwan's public sector and private industries
- **Industrial supply chain vulnerabilities –** Taiwan's prominent role in strategic industries such as semiconductors creates additional vulnerabilities. Cyberattacks targeting major chip manufacturers like TSMC and UMC, key players in the globally connected semiconductor supply chain, can have a ripple effect, impacting global technology giants and disrupting the global economy. TSMC was the victim of a WannaCry ransomware attack, which affected its production lines and caused significant financial losses within TSMC and beyond. Taiwan also dominates the EMS industry with over 80 percent global market share. Major EMS companies like Foxconn, Pegatron, and Wistron manufacture consumer electronics, such as smartphones, laptops, and tablets, as well as industrial and automotive electronics

- **The enemy within –** Insider threats are often overlooked and still pose a significant risk. Whether through inadvertent human error, disgruntled employees or blatant foreign espionage, vulnerabilities are created which malicious actors can exploit. A former employee of a Taiwanese technology firm was arrested for allegedly attempting to sell company secrets to Chinese competitors

Challenges

According to a Taiwan Institute of Information Security (TIIS) 2023 report Taiwan faces a shortage of over 10,000 cybersecurity professionals. The demand for skilled cybersecurity professionals continues to outstrip supply. While awareness campaigns are important, more effort should be focused on developing a robust pipeline of talent. This can include establishing specialised cybersecurity training programmes at universities and vocational schools, in conjunction with upskilling and reskilling of existing IT professionals.

Small and medium-sized enterprises (SMEs) are the weakest link in Taiwan's cybersecurity defence chain and are often overlooked in cybersecurity preparedness efforts. A 2022 survey indicated that 70 percent of Taiwanese SMEs lacked adequate security measures, meaning that they are not prepared if they ever become targets of interest. Many SMEs in Taiwan simply lack the resources or expertise to implement robust security practices.

Public sector initiatives and industry partnerships are needed to provide affordable and accessible training, and provide support specifically customised to SMEs' needs.

The cost of a cyberattack to a Taiwanese SME can be high. The TIIS 2023 study showed the average cost can range from USD 10,000 to USD 50,000 depending on the severity of the attack and the size of the business. TIIS also estimates that an SME facing such attacks will most likely be crippled, potentially leading to partial or whole business closure and job losses.

Many SME owners and employees have limited cybersecurity awareness, making them particularly more vulnerable to malware and malicious code, phishing scams, and social engineering attacks.

The threat landscape is also evolving and therefore cybersecurity defences also need adaptation to meet these threats head on. Having a certain standard of cybersecurity awareness is important, but the public sector and private industry also need to prioritise solutions that address sophisticated cyberattacks and advanced threats employed by nation-state actors and advanced persistent threat (APT) groups. This will require continuous investment in research and development to stay ahead of the threat curve and develop innovative cybersecurity defence measures.

New attack surfaces are being created daily with the proliferation of IoT devices. Regulation and standards are needed to ensure the security of these devices and the data they collect and transmit.

There is also a growing cloud security challenge. As reliance on cloud computing grows, concerns regarding data security and access control in cloud computing environments need to be addressed. Taiwan needs robust regulations and collaborations between the public sector, cloud service providers, and end user organisations to ensure secure cloud adoption and growth.

The rapid rollout of new 5G networks also introduces new vulnerabilities to the mix. Taiwan needs to work closely with technology vendors and international partners to develop robust security protocols for its 5G infrastructure as well as future wireless technologies and infrastructure.

Small and medium-sized enterprises (SMEs) are the weakest link in Taiwan's cybersecurity defence chain and are often overlooked. Limited cybersecurity awareness makes them vulnerable to malware, phishing and other attacks.

Public sector initiatives

Taiwan's authorities recognise the severity of cyber threats and have implemented several initiatives to boost the island's cyber security defences. There are four key programmes or pillars, strengthening institutions and enhanced intra-agency collaboration, investing in education and awareness, building a robust legal framework, and fostering innovation and collaboration.

Established in 2022, the Ministry of Digital Affairs (MODA) has a crucial role in Taiwan's cyber defence strategy. It has the responsibility to promote digital policy innovation and oversees critical cyber security agencies, such as the National Institute of Cyber Security (NICS). Under MODA, NICS spearheads research and development efforts, formulates cybersecurity policies, and provides technical assistance to both public and private sector entities during cyber incidents and escalations. An additional platform, the Executive Yuan (Cabinet) Cybersecurity Council, facilitates collaboration and coordination between central government agencies, local municipalities, and critical infrastructure operators. The platform realises common goals to share information, coordinate incident response, and strengthen overall cyber security preparedness

Name of organisation	Role
Ministry of Digital Affairs (MODA)	Leads Taiwan's digital development, including cybersecurity policy, incident response, and digital resilience. This includes coordinating cybersecurity efforts across government agencies and fostering collaboration with the private sector
National Institute of Cybersecurity (NICS)	Focuses on advancing cybersecurity technology, research, and development. This includes providing technical expertise and support to government agencies and critical infrastructure providers to enhance their cybersecurity capabilities
Executive Yuan Cybersecurity Council	Coordinates and oversees cybersecurity policies and strategies across the government. This includes coordinating responses to cyber incidents, developing national cybersecurity strategies, and allocating resources for cybersecurity initiatives
National Communications Commission (NCC)	Oversees telecommunications and broadcasting in Taiwan, including cybersecurity regulations and the security of telecommunications networks. The NCC sets and enforces regulations related to cybersecurity for telecommunications providers and broadcasters to ensure the security and resilience of critical communication infrastructure

The second pillar of initiatives focus on investing in education and awareness. The authorities launched various island wide cyber security awareness campaigns to educate citizens about the dangers of cyber threats, best practices for online safety, and how to identify suspicious activity. The aims of these campaigns are to equip individuals with a culture of cyber hygiene, and to empower them to be the first line of defence. On the education front, initiatives are currently underway to integrate cyber security into the school curriculum at various levels. The aim here is to equip future generations with the knowledge and skills needed to navigate the digital world safely.

Building a robust legal framework is the focus of the third pillar of public sector initiatives. The Cybersecurity Management Act legislation serves as the cornerstone of Taiwan's cyber security framework. It outlines responsibilities for public sector agencies, critical infrastructure operators, and service providers regarding cyber security protections.

Coupled with the Data Protection Laws, which Taiwan has been actively developing and strengthening to ensure the privacy and data security of its citizens in the digital age, these regulations aim to regulate data collection, storage, and usage practices for both public and private entities.

The final set of initiatives focus on fostering innovation and collaboration. The authorities recognise the crucial role of startups in developing innovative cyber security solutions. There are various programmes that offer funding, mentorship, and industry networking opportunities available to encourage and support promising new ventures in this domain. The authorities also actively encourage collaborations between public and private partnerships, as this is critical for effective cyber defence. Leading technology companies and cyber security experts are frequently consulted to share knowledge, develop solutions, and conduct joint exercises.

Key players

Taiwan's cybersecurity landscape is vibrant and rapidly growing, driven by the increasing number of cyber threats and the widespread adoption of digital technologies. Large and more established enterprises like Trend Micro and TXOne lead the market with comprehensive solutions that protect against a wide range of cyber threats. These companies offer threat defence, cloud security, and cybersecurity services, promising protection for both local and international clients. Their continuous innovation and research into emerging threats help to keep them at the forefront of the industry in Taiwan.

In addition to these larger players, Taiwan is home to a dynamic ecosystem of startups and specialised companies. Companies like Jmemtek, DevCore, and AuthMe focus on niche areas such as hardware-based IC security, AI-driven threat detection, offensive security services, and digital identity verification. These startups bring agility and cutting-edge technologies to the market, addressing specific cybersecurity challenges with innovative solutions. The collaboration between large enterprises and startups helps to foster a robust cybersecurity environment, enhancing Taiwan's overall resilience against cyber threats.

Public agencies / regulators

- 行政院 Executive Yuan
- 國家資通安全研究院 National Institute of Cyber Security
- moda 數位發展部 Ministry of Digital Affairs
- 國家通訊傳播委員會 National Communications Commission

Established companies

- CYCRAFT
- ADLINK
- TREND MICRO
- 中華資安國際 CHT Security
- txOne networks

Start ups

- AuthMe
- DEVCORE
- PUFsecurity
- JMEMTEK
- Urmaz!

Established companies

Adlink Technology

Adlink Technology specialises in edge computing solutions, providing hardware and software for embedded, distributed, and intelligent computing applications. Its products include rugged embedded computers, industrial PCs, network appliances, and software tools, which are used in various industries such as healthcare, transportation, and manufacturing. Adlink's innovations support real-time data analysis and enhanced security.

CHT Security

CHT Security, a subsidiary of Chunghwa Telecom, is a leading cybersecurity service provider in Taiwan, offering a variety of solutions including network security, professional cybersecurity services, and product sales. It serves a diverse clientele, from public agencies to large enterprises and SMEs, providing services like threat intelligence, incident response, and managed detection and response (MDR). CHT Security is recognised for its innovative use of AI and cloud technologies to enhance cybersecurity and for which it has received multiple awards.

Cycraft

Cycraft is a cybersecurity company founded in 2017, specialising in integrating autonomous AI technology to enhance cybersecurity resilience. It provides professional services to public agencies, banks, and high-tech manufacturers across the Asia-Pacific region. CyCraft's platform automates threat investigation processes, such as threat hunting, alert reduction, root cause analysis, and incident response, making cybersecurity more effective and consistent.

Trend Micro

Trend Micro, founded by Taiwanese Americans which became Japan headquartered after a 1992 acquisition of a Tokyo software firm, offers a cybersecurity platform that claims to protect over 500,000 organisations and 250 million individuals across clouds, networks, devices, and endpoints. Trend Micro's solutions include advanced threat defence techniques, cloud security, and enterprise security software for servers, containers, and cloud computing environments. It carries out global threat research and continuously innovates to help ensure protection against evolving cyber threats. As a global company with distributed R&D over 16 locations, Taiwan remains one of its key centres of expertise for technology and human talent development.

TXOne Networks

TXOne Networks specialises in providing OT-native cybersecurity solutions designed to ensure the reliability and safety of ICS and OT environments. Utilising an OT zero trust methodology, TXOne offers both network- and endpoint-based solutions that integrate with existing infrastructures. Its technologies focus on real-time, defence-in-depth cybersecurity, protecting mission-critical devices and networks from cyber threats throughout their entire lifecycle.

Startups

AuthMe

AuthMe is a cybersecurity company that specialises in digital identity verification solutions. Founded in 2019 and based in Taipei, AuthMe offers technologies such as facial recognition, document verification, and liveness detection to help businesses verify customer identities quickly and securely. Its solutions aim to enhance customer experience, reduce fraud, and streamline user onboarding processes across various industries, including financial services, healthcare, and transportation.

DevCore

DevCore is a Taiwanese cybersecurity company founded in 2012, specialising in offensive security services, including Red Team Assessments. It focuses on understanding and simulating hacker methodologies to help enterprises improve their cybersecurity defences. DevCore's team of experts identifies vulnerabilities, conducts advanced penetration testing, and provides strategic recommendations to enhance clients' security postures. Its innovative approach and extensive research into the latest cyber threats helps ensure it stays ahead of potential attackers.

JmemTek

JmemTek specialises in hardware security IP and IC design services, focusing on next-generation hardware security solutions to protect against cyber threats. It integrates security directly into chips, offering comprehensive hardware security modules (e.g., PUF IP) and post-quantum cryptographic encryption algorithms that safeguard data from quantum computing attacks. Its solutions include unique identity authentication, protection of AI algorithms, and true random number generation, making it a key player in semiconductor hardware-based security.

PUF Security

PUF Security, a subsidiary of eMemory Technology, specialises in providing advanced hardware security solutions based on Physically Unclonable Functions (PUFs). Their offerings include PUF-based security IP solutions such as the PUFcc crypto coprocessor and PUFrt hardware root of trust, which are designed to secure semiconductors and connected devices. These solutions enhance security by generating unique, unclonable identifiers for chips, ensuring robust protection against tampering and unauthorised access. PUF Security's technologies are widely used in applications ranging from IoT devices to AI processors, providing comprehensive security from the hardware level up.

Urmazi Networks

Urmazi Networks specialises in Domain Name System (DNS) security solutions, offering products like the iSafer DNS Booster that monitor and control DNS activities to enhance cybersecurity, privacy, and threat visibility. Its technology helps enterprises strengthen network defences against frequent cyberattacks by leveraging a global database for real-time threat intelligence. Urmazi's solutions aim to provide optimal protection for IT infrastructures and hybrid workforces, to help ensure secure online services for both enterprises and their customers.

Opportunity areas for UK companies

Although Taiwan has a vibrant ecosystem of established cyber security companies and young startups, there is always the need to collaborate internationally to stay ahead of the latest zero-day exploits and hostile state APT actors. On a policy level, the previous administration under President Tsai has adopted a strategic approach, emphasising the intrinsic linkage between cybersecurity and national security. The present administration under President Lai will likely continue with this strategy and reemphasise a steadfast commitment to fostering robust international collaboration with allied nations and industry stakeholders, both domestically and abroad.

In the past Taiwan's cyber security partner of choice has been the USA. Noteworthy instances of this collaboration include a joint cyber-war exercise titled 'The Cyber Offensive and Defensive Exercises' (CODE) drills, whose inaugural meeting was held in 2019.

Furthermore, initiatives such as the Talent Circulation Alliance (TCA), established by the Taiwanese authorities in 2019 in conjunction with the American Institute in Taiwan (AIT), have served to facilitate talent exchange and acquisition. The UK has the potential to become another strategic cyber security partner for Taiwan.

UK cybersecurity companies have significant opportunities across various sectors in Taiwan. In the public sector and law enforcement, they can provide advanced threat detection and incident response solutions to enhance security island-wide. In manufacturing and critical infrastructure, there is a demand for robust OT security to protect industrial control systems. The semiconductor and hardware security sector offers opportunities for developing secure chip designs and post-quantum cryptographic solutions. In IT and telecommunications, UK companies can offer comprehensive cybersecurity services to safeguard data and networks. Finally, the finance and banking industries require sophisticated fraud prevention and compliance solutions to protect sensitive financial data and ensure regulatory adherence.

> **"Taiwan is the frontline of digital cyber operations and the eyes for early cybersecurity warnings. The people of both the UK and Taiwan look forward to strengthening collaboration to enhance EU and APAC resilience, leading the way in global cybersecurity innovation and peace of mind."**
>
> Dr Benson Wu, Co-founder and CEO, CyCraft Technology

Public sector and law enforcement

Taiwan's public sector and law enforcement entities are increasingly targeted by sophisticated cyber-attacks, primarily from state-sponsored actors. These attacks threaten critical infrastructure, sensitive public sector data, and law enforcement systems. Taiwan experiences between 20 to 40 million cyberattacks monthly, with a significant portion attributed to suspected Chinese state-sponsored groups. These attacks have exposed vulnerabilities such as outdated systems, a shortage of skilled cybersecurity professionals, and limited inter-agency coordination. Taiwan has recognised cybersecurity as a national priority, leading to the establishment of the National Information and Communication Security Taskforce (NICST) and the National Center for Cyber Security Technology (NCCST) to strengthen its cyber defences. The authorities are actively seeking to enhance its cybersecurity posture through various measures, including the adoption of advanced technologies and international cooperation.

The opportunities for UK companies in cybersecurity for public sector and law enforcement are in:

- **Threat intelligence and automated response systems:** there is a demand for systems that can provide real-time detection and neutralisation of cyber threats. UK companies can offer advanced threat intelligence solutions to help Taiwanese government and law enforcement agencies stay ahead of evolving cyber threats
- **AI and machine learning implementation:** leveraging AI and machine learning can significantly enhance threat detection capabilities, automate response actions, and predict vulnerabilities. These technologies enable a proactive approach to cybersecurity, which is crucial for protecting public sector and law enforcement systems
- **Secure communication and data encryption technologies:** protecting sensitive public sector and law enforcement information from unauthorised access and breaches is critical. UK companies can provide cutting-edge encryption and secure communication solutions to safeguard this data

Manufacturing and critical infrastructure

Taiwan's manufacturing and critical infrastructure sectors are vital to its economy and national security, making them prime targets for cyber-attacks. This creates significant opportunities for UK companies specialising in cybersecurity solutions.

- **Industrial Control Systems (ICS) security**: securing ICS and supervisory control and data acquisition (SCADA) systems is crucial for maintaining the integrity and availability of critical infrastructure. UK companies can offer specialised security solutions tailored to these environments. Conducting thorough assessments to identify and address vulnerabilities in ICS and SCADA systems can help prevent potential cyber-attacks
- **Operation Technology (OT) training:** Taiwan offers several opportunities for training in OT cybersecurity, driven by the increasing emphasis on securing ICS. The Industrial Technology Research Institute (ITRI) collaborates with the International Society of Automation (ISA) to provide certification programmes like ISASecure, which focus on ensuring the robustness of automation and control systems against cyber threats. Additionally, universities such as National Taiwan University of Science and Technology (NTUST or more commonly abbreviated to Taiwan Tech) offer specialised courses in smart manufacturing security and IoT component security, equipping students with the necessary skills to address critical cybersecurity issues in these industries. These initiatives help build a skilled workforce capable of protecting Taiwan's industrial infrastructure from cyber threats. UK companies can work with such entities to exploit these commercial training opportunities
- **Secure communication and data encryption:** protecting sensitive data from unauthorised access and breaches is essential. UK companies can provide cutting-edge encryption solutions to safeguard communications and data within manufacturing and critical infrastructure sectors. Ensuring secure communication channels for critical infrastructure operators can prevent interception and tampering of sensitive information

Semiconductor and hardware security

Hardware security solutions that prevent chips from being hacked, advanced memory technologies, and security solutions for various applications such as security key generation, identification, authentication, and encryption are highly sought after. Using PUF to generate unique and unpredictable random sequences based on intrinsic variations in wafer fabrication is one example. Another example is Arm TrustZone, a security technology that creates two distinct execution environments on a single processor: a secure world and a non-secure world.

The opportunities for UK companies in cybersecurity for semiconductor and hardware security are in:

- **Intellectual property (IP) and design:** UK companies like ARM and Imagination Technologies are highly regarded in Taiwan for their advanced semiconductor IP. Smaller UK firms can leverage this reputation to strike IP licensing deals. There is also demand for innovative design services that can enhance the performance and security of semiconductor products
- **Hardware security solutions:** with the increasing threat of cyber-attacks, there is a growing need for secure integrated circuit (IC) designs that can prevent tampering and reverse engineering. UK companies can offer Trusted Platform Modules (TPMs) that ensure data integrity, confidentiality, and system authentication, which are crucial for protecting sensitive information in semiconductor applications

IT and telecommunications

Taiwan's IT and telecoms industry is rapidly advancing in cybersecurity technologies, driven by the increasing frequency and sophistication of cyber threats, particularly from state-sponsored actors. The sector is supported by public sector initiatives such as the National Cyber Security Strategy, which aims to bolster defences and enhance resilience. Taiwan hosts numerous cybersecurity companies and regularly holds events like CYBERSEC to showcase innovations in areas like Zero Trust Security, IoT, and 5G cybersecurity. Despite these advancements, the industry faces challenges such as integrating new technologies with legacy systems and ensuring compliance with evolving regulatory standards.

The opportunities for UK companies in cybersecurity for IT and telecommunications are in:

- **Network security:** designing and implementing secure network architectures that can withstand sophisticated cyber-attacks is crucial. UK firms can offer solutions that enhance the security of Taiwan's telecommunication networks. Advanced firewall and intrusion detection/prevention systems are essential for protecting IT and telecommunication networks from unauthorised access and cyber threats
- **Data encryption and privacy:** protecting sensitive data from unauthorised access and breaches is essential. UK companies can provide cutting-edge encryption solutions to safeguard communications and data within the IT and telecommunication sectors. Implementing Data Loss Prevention (DLP) solutions to monitor, detect, and prevent data breaches and unauthorised data transfers can help protect sensitive information
- **Quantum communications:** offer a significant opportunity to enhance data encryption and privacy by leveraging the principles of quantum mechanics. Quantum key distribution (QKD), a key technology in this field, enables the secure exchange of encryption keys between parties, ensuring that any attempt at eavesdropping can be detected immediately. This method provides a level of security that is theoretically unbreakable, as it relies on the fundamental properties of quantum particles, such as superposition and entanglement1. As traditional encryption methods face increasing threats from the advent of quantum computing, quantum communications present a robust solution for safeguarding sensitive information in the digital age
- **Cloud security:** as more companies migrate to the cloud, there is a growing need for secure cloud services. UK firms can offer solutions that ensure the security of data and applications hosted in the cloud. Implementing robust Identity and Access Management (IAM) solutions to manage user identities and control access to cloud resources is critical for maintaining security

Finance and banking

The traditional and somewhat antiquated nature of Taiwan's finance and banking industry creates several opportunities for UK cybersecurity companies to introduce modern, robust security solutions. Here are some key areas where UK firms can make a significant impact:

- **Digital transformation and modernisation:** many Taiwanese banks still rely on outdated systems. UK companies can offer solutions to modernise these systems, enhancing security and efficiency. Introducing automated processes can reduce the reliance on manual, paper-based systems, thereby minimising human error and improving security
- **Compliance and regulatory support:** assisting Taiwanese banks in complying with local and international cybersecurity regulations can be a valuable service. UK firms can offer expertise in navigating these regulatory landscapes. Conducting regular security audits to ensure compliance and identify areas for improvement can help maintain robust cybersecurity practices
- **Secure digital banking solutions:** as digital banking becomes more prevalent, there is a need for secure mobile and online banking solutions. UK companies can offer technologies that protect against fraud and cyber-attacks. Implementing robust IAM solutions to manage user identities and control access to banking systems is critical for maintaining security

Success story:
Gorilla Technology (UK)

Gorilla Technology Group Inc. ("Gorilla") is a global provider of AI-based edge video analytics, IoT technologies, and cybersecurity. Gorilla Technology has successfully leveraged opportunities in Taiwan's cybersecurity sector by implementing advanced AI and network intelligence solutions. Its notable projects include a 5G Telecom and Network Investigation Solution for a major Taiwanese law enforcement agency, enhancing criminal investigations and public safety, and an AI Airside Management System at Taoyuan International Airport, which improved security and operational efficiency through video analytics, facial recognition, and license plate recognition technologies. These initiatives have significantly bolstered the cybersecurity and operational capabilities of Taiwan's public sector and critical infrastructure industries.

Routes to market

In addition to the different market entry strategies already outlined above in this report for Japan and Korea, and the options for setting up a local entity, which would apply equally well in Taiwan, British cybersecurity firms can enter the Taiwanese market through several strategic routes:

- Collaborating with the public sector, such as engaging with MODA and participating in national cybersecurity initiatives, can provide access to government contracts and projects
- Forming partnerships with local firms allows British companies to leverage local expertise, navigate regulatory landscapes, and establish a presence in the market more effectively
- Additionally, exhibiting at trade shows and conferences like CYBERSEC Taiwan and HITCON offers opportunities to showcase technologies, network with industry leaders, and explore potential collaborations
- These combined approaches can significantly enhance market entry and growth prospects for British cybersecurity firms in Taiwan.

Public sector collaboration

Working with public sector bodies and central / local authorities' agencies via public tenders or partnerships on island wide cybersecurity initiatives can open doors, but it can be difficult to get started without support and advice. One valuable resource often overlooked by British firms is the Technology Trade Team at the British Office in Taipei (BOT). Its team of experts can arrange access to the relevant authorities and ministries in Taiwan. One financial technology consultant Intralink spoke to said it may take a major failure in some aspect of Taiwan's cybersecurity defences before experienced British cybersecurity companies can fully enter the market. Their experience indicates this is more likely to occur in the banking and insurance industry than anywhere else.

Partnerships with local firms

Entering the Taiwan market through partnerships with local firms offers British cybersecurity companies several benefits, including access to Taiwan's robust tech ecosystem and its strategic position in the Asia-Pacific region. These partnerships can facilitate smoother market entry, leveraging local expertise and established networks to navigate regulatory landscapes and cultural nuances. Additionally, Taiwan's commitment to digital transformation and its strong emphasis on cybersecurity create ample opportunities for collaboration and innovation, enhancing the competitive edge of British firms in the region.

Trade shows and conferences

The main cybersecurity exhibition in Taiwan is the annual Cybersec Taiwan expo, which is the largest of its kinds in Asia. It features over 300 talks, 500+ global brands, and areas like the Cyber Taiwan Pavilion and AIoT & Hardware Security Zone. Other smaller technical conferences are also worth attending, such as the annual Hackers in Taiwan Conference (HITCON), a technology-oriented cybersecurity conference dedicated to bringing the latest and the most in-depth technologies and practices to the security community. In addition, there are other technology related events that feature a large cybersecurity component, such as the Taiwan Cloud Summit, which features online and cloud computing security prominently, and the Semiconductor Cybersecurity Global Summit as part of the annual SEMICON Taiwan event focusing on IC and hardware security.

Cybersecurity events in Taiwan

Event	Date	Website
Cybersec 2025	15-17 Apr 2025	cybersec.ithome.com.tw/2024/en/
Taiwan Cloud Summit 2025	3 Jul 2025	cloudsummit.ithome.com.tw/2024/
Semiconductor Cybersecurity Global Summit	TBD (6 Sep 2024 past event)	www.semicontaiwan.org/en/Cybersecurity_Global_Summit_2024
HITCON (Hackers in Taiwan Conference) 2024	30 Oct 2025	cfp2024.hitcon.org/en/

About this report

This report is prepared as part of the UK-APAC Tech Growth Programme by Intralink Limited.

Exchange rates used in the report

GBP 1 = JPY 199

GBP 1 = KRW 1,770

GBP 1 = TWD 41.5

About Intralink

Intralink is an international business development consultancy specialising in Asia. Its mission is to accelerate companies' growth, innovation and green transition through cost-effective, results-driven global engagement.

The firm has 140+ multilingual employees across 15 offices in Japan, South Korea, China, Taiwan, Singapore, the US, the UK, France, Poland, and Israel.

Its teams on the ground in Asia – immersed in the business practices, cultures and customs of their markets – enable western companies to grow sales and forge partnerships in the region.

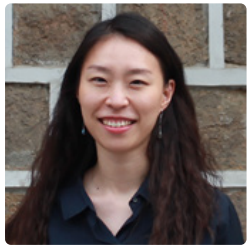
They also help Asian corporates to harness the power of global innovation and governments to grow their exports and attract foreign investment.

Intralink is different from other consultancies in not just developing the right strategies for its clients but taking a hands-on approach to generating commercial outcomes.

Intralink's clients range from startups to multinationals in the medical, energy, automotive, digital media, aerospace, software and other high-growth sectors, as well as government bodies. Many of these organisations are addressing the world's most pressing social and environmental challenges – and Intralink believes that cross-border collaboration will deliver a more prosperous, sustainable society.

Sam Leng
Project Manager

Laura Miyasaka
Project Coordinator



Ha Eun Sohn
Project Manager

Alexandra Gugay
Project Director

Renata Naurzalieva
Director of Operations

About the UK-APAC Tech Growth Programme

The UK-APAC Tech Growth Programme is a government-backed initiative to support the UK's most innovative tech companies' expansion in the Asia Pacific region.

It spans eleven markets: Japan, Korea, Taiwan, Singapore, Vietnam, Malaysia, the Philippines, Thailand, Indonesia, Australia and New Zealand.

Any UK-headquartered technology startups and scaleups keen to develop opportunities in APAC are eligible for the programme.

The goal is to set the companies up for APAC success by helping them:

- Understand if there is an opportunity – and learn how to approach the region
- Validate which potential customers and partners will be interested in their technology – and get the customers' eyes on their product
- Accelerate in-market opportunities, secure partnerships and lay the foundations for commercial success in the target market(s)

Depending on the participants' readiness level, they can be selected for a wide range of free or subsidised activities – from business matching with major corporates to overseas missions, pitch events and bespoke in-market business development initiatives.

The programme is a joint initiative led by the Department for Business and Trade, the Department for Science, Innovation and Technology and Intralink.

UK-APAC Tech Growth Programme

Northeast Asia's cybersecurity market – opportunities for UK companies

The information contained herein has been obtained from sources believed to be reliable, but is not guaranteed as to its accuracy or completeness. An effort has been made to go beyond simple data collection in this report: responses have been interpreted to elucidate the underlying processes, motives and relationships involved in the dynamics of the situations under investigation.

All references to factual data and properties should be recognised as respondents' perceptions of reality unless otherwise stated.

This report is not intended for, and should not be used as, an investment recommendation.

www.intralinkgroup.com

Intralink

Funded by UK Government