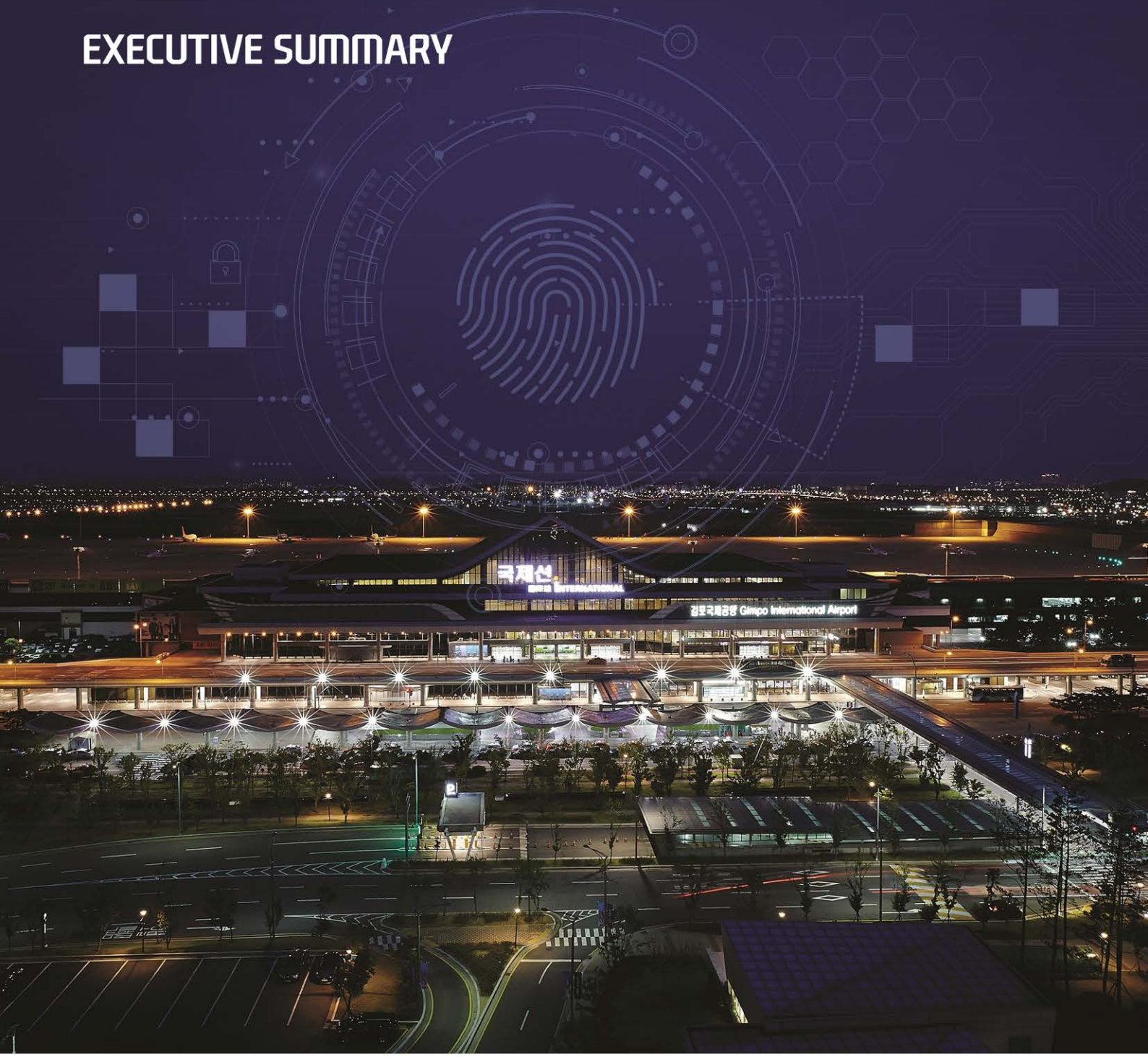
KOREA AIRPORTS CORPORATION

CYBERSECURITY MANAGEMENT PLAN IN RESPONSE TO SMART AIRPORT PROMOTION

Dohee KIM
Manager
Cyber Security Center
Korea Airports Corporation

CONTENTS

EXECUTIVE SUMMARY



Airports are undergoing rapid digital transformation marked by the enhancement and expansion of operational information systems and the introduction of new systems, paving the way for smart airports. Airport operations face a growing exposure to the internet, necessitating increased protection for airport operational systems against cyberattacks. Addressing cybersecurity concerns and managing vulnerabilities post-construction of operational systems and during service operations pose challenges. Hence, it is imperative to incorporate information security considerations from the outset of system construction.

TO ADDRESS THESE CHALLENGES,

CHAPTER 1

Proposes a security management plan for each stage of system construction.

Constructing an airport operation system with a focus on information security is crucial from the design stage onward. During the operational phase, stringent management of outsourced service providers residing for the system construction project is essential, and conclusion of construction involves thorough checks for software development security vulnerabilities and server vulnerabilities, ensuring information security across the construction lifecycle from inception to completion.

CHAPTER 2

Focuses on cultivating a culture of cybersecurity awareness.

Cybersecurity is a collaborative effort involving all employees including the cybersecurity department. The most impactful method for enhancing employee cybersecurity awareness is integrating cybersecurity activities into departmental performance evaluations for heightened awareness and enhanced airport cybersecurity.

CHAPTER 3

The focus is on countering external intrusions.

As multiple airport facility networks evolve, firewalls are employed to prevent access between networks, yet there are limitations to the effectiveness of current firewall responses. The deployment of next-generation firewalls, complemented by logical firewall configurations, can efficiently prevent unauthorized access. Furthermore, AI-based detection and response systems can automatically block attackers with high malicious scores through external reputation checks.

CHAPTER 4

Addresses insider security management,

specifically incidents of data leaks Involving service companies. Key strategies include reinforcing network access control through an Information Asset Management System (IPMS) and establishing strengthened server access control system, network-linked data transmission system, and a USB control system to enhance insider information security.

CHAPTER 5

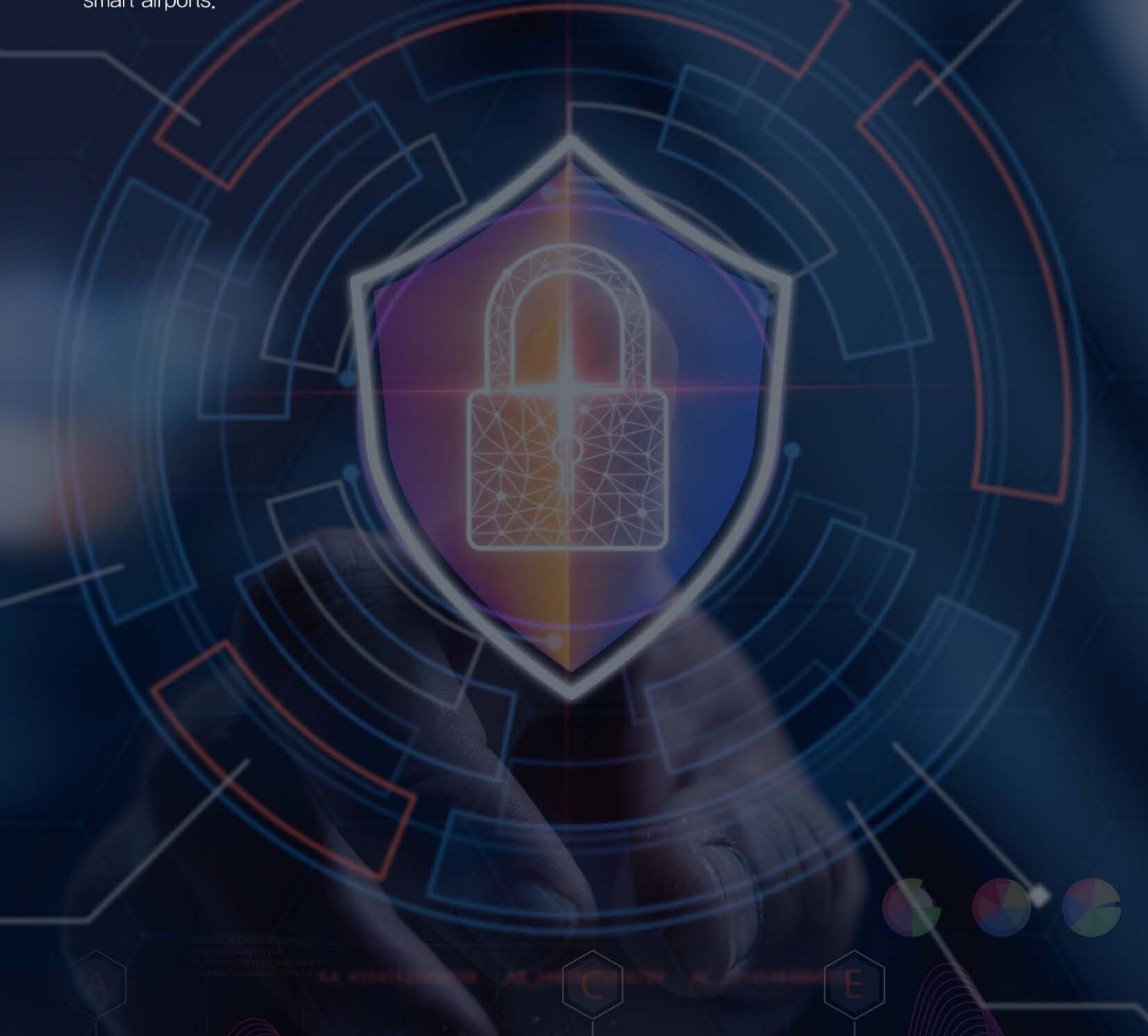
Focuses on the management of personal information within airports.

Airport operational information systems, containing personal data of various stakeholders including Korea Airports Corporation (KAC) employees, its subsidiaries, and service companies, require tailored alignment with the airports' unique operational context. When airports store biometric data for identification, it is essential to implement suitable privacy measures.

Given the unique characteristics of these airports, this paper aims to establish a cybersecurity culture within airport operations. This involves collaborative cybersecurity management with stakeholders, implementing comprehensive cybersecurity management strategy encompassing the prevention of external intrusions and insider leaks, and ensuring secure and stable airport services through management of personal information within airports.

INTRODUCTION

As digital transformation accelerates, the expanding scope of cyber threats heightens the significance of cybersecurity. The aftermath of a cyber breach extends beyond specific companies or individuals, causing national-level losses. In Korea, cyber incidents increased from 130 in 2017 to 145 in 2018 with costs rising from $1.17 million to $1.3 million, indicating a potential future surge (A study on Economic and Social Cost Estimation of Cybersecurity Breaches, p. 22). Airports, crucial for national security, basic livelihoods, and economic stability, face a rising number of cybersecurity incidents. However, allocating budget and personnel to cybersecurity is challenging due to prioritization of primary functions. Constructing and operating new airport systems for enhanced customer convenience poses a challenge in raising cybersecurity awareness when KAC and its contractors lack a dedicated cybersecurity management system. Awareness is often viewed solely in the context of airport services, highlighting the need to increase awareness among stakeholders and develop a cybersecurity management plan for smart airports.



01

SECURITY MANAGEMENT MEASURES FOR EACH STAGE OF SYSTEM CONSTRUCTION

01 | Security Management Measures for Each Stage of System Construction

Integrating security considerations from the planning stage is crucial for information security in airport operational systems. Retroactively addressing vulnerabilities after the system is constructed is costly and poses constraints. Active support from the cybersecurity management department is vital, especially considering potential cybersecurity unfamiliarity in business management overseeing system construction.

Planning stage

Comprehensive security review should be conducted. This involves scrutinizing cybersecurity measures in informatization including network configuration, introduction of equipment with verified cybersecurity features, and the handling of personal information. Additionally, the safety and test certification of new information protection system security functions require verification. Security training for software developers should be implemented to prevent source code vulnerabilities. Continuous assessments using the software development security check program should be conducted to address identified vulnerabilities.

Operational stage

If outsourced service provider's employees bring a PC for business and connects to the intranet and Internet network, it poses a potential risk of virus infection or data leakage. When bringing in equipment, they must use clean PCs with no unauthorized files or programs. Employees of the service provider must sign a non-disclosure information security pledge. Maintaining a data ledger for borrowed and returned business materials is crucial to prevent leaks. Mandatory weekly PC inspections by the service supervisor is implemented with cybersecurity department verification through on-site checks by a designated person. It's essential to block wireless AP functions, install PC security programs, and conduct periodic checks for service company's compliance with security regulations. Installing an automatic document deletion program on Internet-connected PCs prevents retention of work materials by deleting materials upon PC shutdown and restart. For data security, using a proven complete wipe program is advised over Windows' formatting feature when taking a PC out of the office to avoid potential work data recovery through recovery programs.

Completion stage

In the construction's final phase, a thorough source code vulnerability check is needed due to the increasing prevalence of cyberattacks exploiting software vulnerabilities, particularly targeting vulnerabilities before security patches are released, as observed in zero-day attacks using unknown vulnerabilities and web hacks. Implementing source code vulnerability scanning is essential to minimize developer mistakes and errors, reducing external cyberattacks. Running an airport operations information system without addressing source code vulnerabilities may result in cybersecurity breaches. Aligning source code vulnerabilities primarily with software development security practices and conducting periodic checks using a security program is necessary. Thorough oversight of outsourced service providers, from initiation to completion, is vital.

02

RAISING AWARENESS AND CULTIVATING A CYBERSECURITY CULTURE

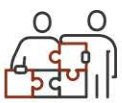
02 | Raising Awareness and Cultivating a Cybersecurity Culture

Enhancing cybersecurity goes beyond costly information protection systems. It requires active employee involvement, collaborating with airport stakeholders to fortify cybersecurity measures. Achieving this objective entails fostering awareness among employees and establishing a cybersecurity culture with airport stakeholders.

Departmental performance evaluation

To nurture a cybersecurity culture at airports, the cybersecurity activity index can be integrated into internal evaluations. In KAC, assessing departments are based on PC security inspection scores, and results from simulated hacking email response drills. The index can be customized for each airport's cybersecurity priorities. For instance, if the server operating system (OS) updates managed by the airport are not kept current, the prioritization of server operating system updates is enhanced, assigning them greater significance in the scoring system. KAC operates multiple airports, and each department within them actively engages in cybersecurity activities for high internal performance evaluation scores. Under this cybersecurity management, KAC cultivates awareness and promotes a vigilant culture among all employees. Due to the lack of dedicated cybersecurity personnel at airports and the general absence of cybersecurity expertise among employees, addressing vulnerabilities and implementing necessary measures is challenging. Therefore, the headquarters' cybersecurity department undertakes the responsibility for regular checks and proposes improvement measures. The current inspection prioritizes the airport facility network due to its growing significance with various information systems emerging in fields such as navigation, machinery, and electricity due to digital transformation. System overseers often solely focus on airport services, necessitating continuous security checks and awareness promotion. First, it is essential to identify the information system assets of the facility network through port scan. Managing the current status of information systems is crucial and fundamental to assess protection needs. Inadequately identifying asset status could cause a cyber breach on airport operational equipment without the responsible person's knowledge. Identifying the current status should be followed by ensuring security measures for each server. Additional measures include blocking unnecessary service ports, deleting or changing default administrator accounts, applying the latest security patches, installing PC security programs, blocking unauthorized wireless AP use, and using authorized USBs. With increased security risks in the facility network nowadays, on-site inspections at each airport are essential for improvement.

Listening to voices of stakeholders



One obstacle to fostering a cybersecurity culture is employee inconvenience due to the annual increase in airport operation information systems and information protection systems. The construction of such systems may complicate procedures or block services, affecting work efficiency. Balancing this requires regular monitoring to avoid excessive measures. Addressing this challenge involves gathering feedback on information security inconveniences from airport employees to identify and improve procedures. While the cybersecurity department prefers stronger measures, other departments prioritize work convenience. Bridging this gap involves regularly collecting opinions and establishing a cybersecurity system considering business convenience, ensuring active employee participation. Neglecting this misalignment can cause dissatisfaction and hinder a comprehensive airport-wide cybersecurity culture.
It is essential to consider opinions that may include concerns about unnecessary procedures and inconveniences following new system implementation.

Bug bounty

With the yearly increase in airport operational information systems, the cybersecurity department faces the challenge of regularly checking and securing all systems. A single vulnerable system can become an entry point for a cyberattack. Despite having enough personnel for vulnerability scanning, consistently assessing and enhancing security for hundreds of systems remains challenging. To address, encouraging all employees to participate in bug bounties can leverage collective knowledge with points integrated into the cybersecurity activity index (as mentioned in Departmental performance evaluation section) for employee involvement. Additional points can consider potential system impact, cyberattack complexity, and difficulty of discovering vulnerabilities. Regular incremental training, ranging from basic information system vulnerability checks to advanced remediation, fosters a cybersecurity culture. Bug bounties complement traditional vulnerability scanning, allowing average employees to identify simpler security vulnerabilities across broader systems. It is advisable to focus bug bounty submissions on systems not directly managed by the submitting department. This is to prevent intentional withholding of vulnerabilities for later bug bounty points. Proactive measures should preempt such occurrences.

Information security disclosure

Information security disclosure cultivates a cybersecurity culture by affirming customers' right to be informed about the airport's cybersecurity. With cyber breaches in Korean companies including the compromise of customers' personal information, property damage, and service disruptions, customers now weigh service providers' cybersecurity levels before using their services. Disclosing airports' cybersecurity details to stakeholders minimizes information asymmetry, bolsters external credibility, and builds customer confidence. Careful and selective disclosure is paramount due to public availability, allowing stakeholders to objectively assess the airport's cybersecurity. Key disclosure items may include information security investment, personnel composition, certifications, and activities. Beyond internal awareness, external promotion among stakeholders enhances airport's cybersecurity culture.

Information security consulting

Neglecting cybersecurity during airport system design increases vulnerabilities and escalates later improvement costs. Consulting provides step-by-step guidance from design to operation, eliminating security issues with new system construction. Often, airport operation departments reject information security audits due to perceived penalties. Information security consulting addresses deficiencies and resolve grievances without penalizing working departments. Consulting on network configuration and secure information system during the design phase, and conducting security inspections for outsourced on-site service providers during their residency enhance cybersecurity awareness among less-experienced employees in airport system construction, strengthening airport cybersecurity.

03

RESPONSE TO EXTERNAL INTRUSIONS

03 | Response to External Intrusions

Confirmed North Korean-origin cyberattacks on the public sector of South Korea now average 1.5 million per day, with an expected rise. The initial 1.3 million attempts recently increased approximately 200,000. Such a unique environment allows for specific measures to counter external cyberattacks and safeguard airport systems effectively.

Next-generation firewall

In constructing airport systems and new networks for digital transformation, incorporating next-gen firewalls is essential to counter sophisticated cyber threats. Next-generation firewalls consolidate security measures into a single device, eliminating inefficiencies of individual firewalls and facilitating real-time network traffic analysis. Unified firewall policy management strengthens airport network security as opposed to fragmented management. The evolving speed of attacks on information system assets, such as servers and PCs, are evolving, poses challenges for manual tools. Consolidating physical firewalls into a logical firewall for strategic deployment in specific network segments can create a network security environment optimizing efficiency. This enhances operational efficiency and ensures policy consistency, strengthening airport network security.

AI-based detection and response system

Rising automated cyberattacks, resulting in a surge of security threats and unknown hacking incidents, challenge conventional protection systems relying on predefined patterns for blocking. AI-based systems, leveraging data from firewalls and IPS, effectively counter increasingly automated cyberattacks with limited resources. They create training datasets to evaluate risks, improving accuracy with an expanding network. AI correlates and analyzes logs for identification and counteraction of threats evading security personnel. Synergizing with next-generation firewall section for automated detection and blocking enhances effectiveness. The AI system identifies advanced threats, relays information to the firewall, and automatically blocks them, categorizing them as cyber threats. Crucially, it prioritizes blocking only assessed high-risk attacks to prevent false positives, ensuring uninterrupted airport services. Using big data analytics and AI learning enables identification of previously undetectable cyber threats and swift responses to unknown threats.

Backup and recovery

In recent years, Korea has experienced disruptions like data center fires and network failures, causing significant service interruptions. Disasters, cyber terrorism, server overloads leading to paralysis, or ransomware infections in critical facilities such as airports may inconvenience customers and pose safety risks. In events of a fire or power outage causing server paralysis, a robust backup system is crucial. The first step involves prioritizing information system recovery by identifying systems for immediate restoration with relevant personnel collectively assessing each system's importance. Priorities are established by analyzing factors such as (1) the impact, (2) crucial information presence, and (3) external system interconnectedness. After formulating a backup and recovery plan, thorough testing during non-operational hours evaluates real-world effectiveness and identifies areas for improvement.

Cyberattack response exercises

To effectively counter actual cyberattacks, realistic cyber response exercises are essential. Training on various scenarios enhances organization's threat-handling capability. There are five drill types.

The first drill focuses on Distributed Denial of Service (DDoS) attacks.
While backup and recovery procedures are crucial for mitigating the impact of a DDoS attack that may overload and paralyze the system and network, robust DDoS response systems are the best defense. Simulating various attack scenarios including bandwidth exhaustion attacks (ICMP flooding) evaluates defense effectiveness. Simulated attacks' intensity and duration are gradually increased to validate response capabilities.
If inadequate, connecting to a DDoS shelter service can be considered. KAC subscribes to a domestic telecommunications company's service. In case of traffic surges beyond the response equipment's capacity, the corporation switches to the shelter service's proxy IP provided by the telecommunications company or government agencies for a second and third line of defense.

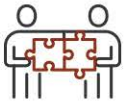
The second type is a mock hacking email drill addressing the frequent threat of hacking emails to employees. KAC sends training emails to all employees using its own mock hacking email sending system, educating non-reporting employees. The training emails are sent with subject lines based on social issues and work-related content to stimulate curiosity. Non-reporting employees face penalties in performance evaluations, emphasizing the need for biannual training to enhance response capabilities.

The third type is a network penetration drill, using deliberate hacking simulations targeting the corporation's public services including its website. It assesses the appropriateness of security and information protection system policy and take follow-up measures for found vulnerabilities. Unlike normal checks, it involves a Red team for attacks and a Blue team for defense. The defense team conducts cyberattack defense without being provided any info on the attack team. The attack team executes scenario-based network penetration, web mock hacking, and information leakage attempts. Port and web scanning, focusing on prevalent cyberattacks and global vulnerabilities from the past three years, generate prompt remediation.

The fourth type is a tabletop exercise with incident details emphasizing response at each stage of a cyber crisis. The goal is to foster an organic response, preventing the spread of damage. It is segmented into a crisis alert drill and an incident situation drill. In the former drill, participants create a report for varying threat levels of attention, caution, alert, and seriousness. Incident situation drills involve responding and taking action based on reports of a fictitious incident and the provided situation message. The attention phase intensifies cyber threat detection, the caution phase enhances threat responses, the alert phase requires coordinated efforts, and the severe phase addresses national-level crisis scenarios. These drills enable a review of the situation and response at each stage of a cyber crisis warning.

The fifth type is a cyberattack defense exercise.
In KAC, the network penetration drill involves the internal cybersecurity team while the defense drill collaborates with other public institutions.
This assesses defense capabilities against real-time attacks, establishing an authentic network environment. It leverages cybersecurity technologies such as web security, digital forensics, reverse engineering, and cryptography and involves competition within a set time limit, with higher scores awarded for resolving problems either the most or the fastest. KAC actively engages in cyberattack defense drills with other public institutions at least biannually. These drills provide insights into real hackers' thought processes, improving KAC's ability to respond to cyberattacks.

Collaborative security control with stakeholders



KAC has a dedicated cybersecurity control room to counter cyber threats, collaborating with the control centers of governmental entities such as the National Intelligence Service and the Ministry of Land, Infrastructure, and Transport (MOLIT) to counter cyberattacks.

This joint initiative allows government agencies to address cyberattacks not detected by KAC's systems. The three-tiered cyberattack detection and prevention system-national security control (NIS), sectoral security control (MOLIT), and unit security control (KAC) -strengthens collective response capabilities.

Moreover, the government actively combats cyber threats by sharing the latest domestic and international security trends, vulnerabilities, cyberattack information, up-to-date advisories, and detection rules through a government-run information sharing system titled "Korea Cyber Threat Intelligence".

As of January 1, 2023, 326 public institutions* used this system to exchange diverse cybersecurity content, strengthening nationwide measures (*2023 National Cybersecurity White Paper, p. 25).

04

INSIDER SECURITY MANAGEMENT

04 | Insider Security Management

Given the rise in cybersecurity incidents involving on-site outsourced providers, enhancing insider security is vital alongside preventing external intrusions. Internally, implementing step-by-step security authentication for employee access enables identifying risks in advance and verifying new access, establishing a zero-trust insider security management plan that mistrusts everyone.

Information property management system

The system is a network security management system that links NAC (Network Access Control), which blocks network access of unauthorized terminals and information security violations, and the information property management system automating network resource registration and reallocation. Managing the increasing number of PC terminals becomes challenging for cybersecurity personnel. When numerous PCs are connected in a short time, DHCP (Dynamic Host Configuration Protocol) facilitates automatic IP assignment and network access control, eliminating the need for manual IP assignment and authorization for each PC to connect to the intranet. Implementing this system with systematic information asset management, automated approval or rejection of network access, and network failure analysis builds an efficient and reliable network security management system, enhancing employee convenience and cybersecurity.

Server access control and account management solution

Security incidents from insider misuse, include indiscriminate access, inadequate account/password management, insider malfeasance, and delays in analyzing the cause of and recovering from the incident. Proactive control and reactive auditing through server access control and account management solutions address these issues.

The first feature is access control employing two-factor authentication including access equipment, access period, command permissions, OTP, and SMS for server access accounts. It also includes permitting the use of designated IP only at the designated time and blocking unauthorized commands instantly.

The second feature involves real-time session monitoring, capturing all server access user actions in video format for post-incident analysis. This allows identifying the cause of an incident.

The third feature automates account management, blocking unauthorized accounts and managing passwords automatically, eliminating the need for manual changes to passwords of numerous accounts every 90 days.

The fourth feature introduces fine-grained access control, limiting server access to essential functions. It blocks unused commands during server access, and if unnecessary access is granted even after work completion, it is automatically rejected. Given the imperfection of insider trust, establishing access control policies is vital for bolstering insider cybersecurity. Centralizing control and automating account management for airport operations reduces time and costs, boosts efficiency, and strengthens information system access control.

Physical network separation and work data transmission

The most reliable method to protect work data is to block data leaks on the Internet by physically isolating the intranet from the Internet and using two PCs per person. This helps prevent ransomware infection through the Internet. For importing or exporting work files, a network-linked data transfer system should be used, reserving Internet-connected PCs for browsing.
Malware-susceptible files like exe and msi should be blocked through network-linked data transmission, with exceptions for necessary business purposes.
Infected documents should be cleaned before being brought inside.
When work files are taken outside, a privacy detection solution is used to identify potential personal information, allowing employees to review and delete as needed.
For files transferred to the Internet network, generic email domains like Gmail and file-sharing sites should be restricted, using dedicated webmail exclusively for data transfer with monitoring and protection measures in place for all work materials sent via dedicated webmail.

USB control

To prevent virus spread via airport PCs, essential USB security measures are crucial. PCs linked to vital airport facility systems require scrutiny due to potential malware damage and prevalent USB-related hacking threats.
Unauthorized data disclosure, coupled with creating network contact points through wireless LAN cards in USB form, poses a risk of cyber breaches. Implementing a USB control system becomes essential to prevent such incidents.
This system restricts unauthorized USB use, ensuring authorized USBs remain internal and can be password-protected for enhanced security. Regular monthly USB checks remove unnecessary materials and periodic management of unused USBs is facilitated.
In case multiple USB devices are used, it is recommended for each department to keep a record using a USB management ledger.

Document centralization system

Integrating and managing all employees' work data on a single server prevents data leakage, without the need of individual PC storage.
During information system construction projects, outsourced service providers use external PCs to store project data and should delete the data upon project completion. But they often fail to comply, with still having the data. A document centralization system mitigates this risk by storing all work materials in one secure location.
In the era of increased remote work during the pandemic, employees may use personal PCs to access the company's business system. A document centralization system enables seamless work processes on personal PCs, eliminating the need to take work materials home and is advantageous in the non-face-to-face work environment.

05

PRIVACY MANAGEMENT IN AIRPORT INFORMATION SYSTEMS

05 | Privacy Management in Airport Information Systems

The EU's GDPR (General Data Protection Regulation), enacted on May 25, 2018, highlights the global need to protect personal data. Given airports' data-rich systems, managing privacy is crucial. KAC's airports collaborate with the Personal Information Protection Commission and conducts regular audits for administrative and technical safeguards.

Administrative safeguards

Processing personal information involves four stages: collection, use, provision, and destruction.

During the collection, the airports gather minimal needed personal information, following timeframes and business needs. Obtaining data subject's consent becomes crucial in the absence of a legal basis.

The second phase phase verifies usage alignment with the initial purpose, ensuring encryption of crucial information like resident registration numbers.
If personal information is employed for additional purposes, prompt elimination of the info and renewed consent are imperative.

In the third phase, it's important to secure the data subject's explicit consent to third parties. Additionally, there should be a legal foundation justifying disclosure without consent.

The fourth step is entrusted processing, involving overseeing and training firms entrusted with handling personal information. Training all involved personnel is essential to impart the significance of safeguarding personal information by external entities.

The fifth phase is instant destruction upon fulfilling the purpose or concluding the retention period. To prevent personal information persistence in the database beyond the retention period, automatic destruction is advisable.

Technical safeguards

Technical measures complement administrative measures in safeguarding personal information.

The initial focus is on access rights management, tailoring access levels to individual data processors' responsibilities. Access rights should be granted according to job duties to the minimum extent required for task performance and restricted promptly for personnel changes such as retirements. Maintaining access rights records for three years and analyzing logs during incidents are essential. Adhering to the "one person, one account" principle prevents account sharing, promoting effective log analysis and tracking during security breaches. Passwords for processor accounts must meet criteria, consisting of at least 9 characters with a combination of letters, numbers, and special characters. Auto-lock passwords after five failed attempts is needed to thwart brute force attacks.

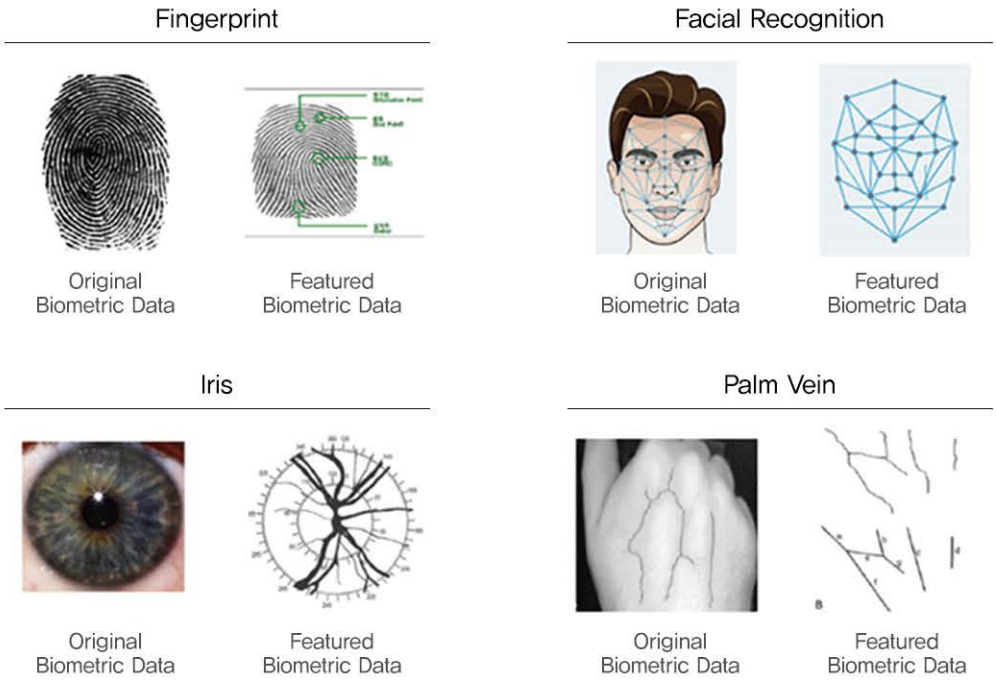
The second aspect involves access control to permit only authorized users in the personal information system, using PC IP and MAC addresses. It is advisable to implement access restrictions based on these addresses for each account. This ensures that even if an account is authorized, it will be restricted from accessing IPs other than the specific one assigned to it. Setting session timeouts to auto-logout accounts after 30 mins of inactivity prevents unauthorized access during user absence.

The third element pertains to personal information encryption.
Despite deploying various protection systems, preventing all external penetration is challenging. Therefore, it is essential to encrypt vital personal information to guard against potential leaks, rendering breached personal information unusable. Two types of encryption exist: two-way for decryptable business information such as resident registration numbers, passport numbers, and biometric data and one-way for information that does not require decryption like passwords. When implementing encryption, it is safe to use algorithms like SEED, ARIA, and LEA for two-way encryption, and SHA-512 for one-way encryption.

The fourth measure involves maintaining and scrutinizing access records, which are indispensable for investigating incidents of personal information leakage or misuse. They include actions by data processors when accessing the processing system, account details, access dates, IPs, processed data subject information, and tasks performed (e.g., inquiry, modification, deletion, addition). Logs should be retained for over 2 years for critical systems and over 1 year for others with regular monthly checks to detect any potential misuse, loss, theft, or leakage. Anomalies require investigation into the processor's standard business conduct. Abnormal behavior mandates corrective measures such as education and recurrence prevention for the processor.

Biometric information protection

The airport's access control system for protected areas and passenger identification system store biometric data such as vein patterns and fingerprints for operation, posing risks if leaked. To mitigate these risks, only essential biometric features for identification, not the original data, are stored. The original data used for biometric feature extraction is promptly destroyed. When storing biometric data in a database, a recommended practice is to split it into two databases, ensuring even if one is compromised, the information remains unusable without the data from the other database. Technical methods verify biometric data by extracting features from the original data.



Source: Biometric Information Protection Guidelines, p.5 (Personal Information Protection Commission, September 2021)

Secure storage of biometric data is critical to prevent leakage or misuse during collection, transmission, and storage. Implementing security measures is essential, given the difficulty in recovering from the potential breach. Diverse security protocols exist to safeguard biometric data throughout its lifecycle.
First, it is essential to assess the necessity of biometric data and whether collecting such data is vital for airport services.
Second, establishing alternatives is crucial when a data subject opts not to provide biometric information.
For instance, if someone declines fingerprint data, airports can implement ID card procedures for identity verification.
Third, it's advisable to use measures like temperature detection, pulse analysis, and skin electrical resistance to counter fake, tampered biometric data and prevent unauthorized use.
Fourth, it's vital to encrypt biometric data during transmission or storage to prevent hacking attempts even if the information is intercepted.
Finally, it's important to promptly dispose of biometric data when the retention period expires or the processing purpose was fulfilled.

Airport CCTV management

Airports deploy a higher number of CCTV systems for security compared to other facilities, necessitating strategically placed signs in customer–visible areas due to the inherent privacy risks of the involuntary recording of personal video information.
CCTV signs communicate installation purpose and locations the responsible personnel details. Voice recording through CCTV is strictly prohibited, and network separation prevents external intrusion. Periodic scans of the CCTV network service ports and cybersecurity addresses potential vulnerabilities. When formulating the CCTV operation policy, it must include installation rationale and purpose, quantity, locations, management personnel, storage duration, and technical and administrative measures.
For footage requests in criminal investigations or lost belongings, following procedures are observed. Data subjects can request access to personal video information while third parties must provide a legally supported letter for access.
After confirming requester's identification, the content, and storage status, requested videos are masked to exclude other individuals' personal video information before provision and footage is promptly destroyed once the request's purpose is fulfilled.

CONCLUSION

Recognizing airports' vital role in people's lives, it is imperative to implement robust cybersecurity measures to ensure safety. In the unique context of Korea's susceptibility to cyber threats, KAC actively collaborates with stakeholders including government agencies such as the NIS and the MOLIT.

This collaboration involves analyzing and sharing cybersecurity threat information, fostering a collective response. Moreover, KAC remains vigilant in overseeing the cybersecurity of its subsidiaries and outsourced service providers.

Committing to cybersecurity, all employees actively engage in cybersecurity activities, aligning with the distinctive characteristics of airport operation systems.

This commitment extends to creating a cybersecurity management plan aligned with smart airport initiatives, which further strengthens airport cybersecurity and fosters a cybersecurity culture.

REFERENCES

01
https://www.kisa.or.kr/20303/form?postSeq=12003&lang_type=KO (2023 National Cybersecurity White Paper (Korean))

02
https://www.kisa.or.kr/402/form?postSeq=2244(2023 Information Security Disclosure Guidelines)

03
https://www.kisa.or.kr/201/form?postSeq=12065&lang_type=KO&page=1 (A Study on Economic and Social Cost Estimation of Cybersecurity Breaches, December 2021)

04
https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleDetail.do (2022 Guidebook on EU GDPR for Korean Companies)

05
https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95 (Personal Information Protection Act)

06
https://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000229672 (Criteria for Implementing Measures to Safeguard the Security of Personal Information)

07
https://www.kisa.or.kr/2060305/form?postSeq=5&lang_type=KO (2018 Guide to Cryptographic Algorithms and the Lengths of Cryptographic Keys)

08
https://www.etnews.com/20231101000363 "Cyberattack Attempts Originating from North Korea on South Korea Averaging 1.5 Million Per Day"

09
https://www.kisa.or.kr/2060204/form?postSeq=5&lang_type=KO&page=1 (Software Development Security Guide (December 29, 2021))

10
https://www.bugbountyclub.com/beginning

11
https://www.kisa.or.kr/2060205/form?postSeq=20&page=1 (Executive Summary of Zero Trust Guidelines 1.0)

12
https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7529 (Biometric Information Protection Guidelines (September 2021))

13
https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7260 (Guidelines for the Installation and Operation of Image Data Processing Equipment in Public Institutions (April 2021))