Science and Technology Trends
Governance Systems for Cybersecurity

Cybersecurity Policy and Governance in Korea: A Close Look at "Authentication" †

Hyeon-Suk Lyu

1. Introduction

In the past few years, a number of incidents involving large-scale disclosure of personal information have occurred in telecommunication companies, as well as in public departments and agencies in Korea. These incidents have raised people's awareness of personal information protection and caused social anxiety and distrust. As a representative case, the personal information of over 100 million people, which belonged to three major credit card corporations, was inadvertently disclosed in January 2014 (Financial Supervisory Service, 2014: 31). According to the report (2014), "Current State of Personal Information Leakage in 2010-2014," published by the Korea Communications Commission, the personal profiles of 106.2 million people were leaked over a four-year period.

It is well-known that most cyber infringement incidents involve the disclosure of personal information, which is related to the process of authentication (Otto, P. N. et al., 2007). The identity theft occurred while collecting citizens' resident registration numbers, which is similar to a Social Security Number in U.S., in order for websites to identify users online. As a result, the ban on collecting resident registration numbers online was included in the Privacy Protection Act of August 2014. No corporation, including one-man companies and public companies, is permitted to gather the resident registration number except in exceptional situations as defined by the law.

The public's awareness of the significance of personal information protection, however, is still lacking; they believe that their personal information has already been leaked to varying degrees, and that policies for cybersecurity would not work properly (Malandrino, D. et al., 2013: 280). This distrust is attributed to the current status of cyberspace, which remains vulnerable to attack and manipulation from ever-evolving malicious threats. Cyber-attacks and crimes are currently the fastest growing threats to almost every aspect of modern life, from the government to the private sector. New cyber-attacks such as DDoS, malicious apps, pharming, smishing, APT, etc. are also rapidly expanding across the world. In addition, with technological advancement and convergence such as ICBM (Internet of Things, Cloud, Big Data, and Mobile), complexity, uncertainty,

Korea Institute of Public Administration, 235, Jinheung-ro, Eunpyeong-gu, Seoul 03367, Korea
E-mail: hslyu@kipa.re.kr

† This article is a modified version of an excerpt from Lyu, H.S. et al. (2015). A Study on Cybersecurity Policy and Governance in the ICT Convergence Environment: Focused on "Authentification". KIPA Research Report 2015-24.

and risk in the cybersecurity environment are ever increasing. As stated above, it is well-known that the majority of cybersecurity incidents take place due to personal information disclosure. According to FIDO alliance (2015), 76% of cyber incidents occur in the process of authentication.

However, South Korea's cybersecurity institutional arrangements and corresponding government policies do not seem to address these issues and challenges in a timely and appropriate manner. This is due to a lack of inclusive legislation, an effective governance system, budget, etc. More specifically, the existing legislative system pertaining to cybersecurity includes the "Digital Signature Act," "Electronic Government Act," 'Framework Act on National Informatization," "Act on the Protection of Information and Communications Infrastructure," "Act on Promotion of Information and Communication Network Use and Protection of Information," "Framework Act on Electronic Commerce," and "National Cybersecurity Management Regulation (Korea Communications Commission, 2011)." These laws show that various roles in protecting personal information are scattered across multiple departments (see Table 1). For instance, "Digital Signature Act" pertaining to authentication certificate authorizes the Ministry of Science, ICT and Future Planning. "Electronic Government Act" and "Electronic Financial Transaction Act" authorize the Ministry of Government Administration and Home Affairs and Financial Services Commission respectively.

Table 1. Agency and law related to authentication

<table>
<tr><th>Sector</th><th colspan="2">Public Sector</th><th colspan="2">Private Sector</th></tr>
<tr><td>Establishment of Policies for Personal Information Protection</td><td colspan="4">• "Framework Act on National Informatization": Information Security Professional Committee
• "'Act on Promotion of Information and Communication Network Use and Protection of Information": Establishment of information protection policy</td></tr>
<tr><td>Protection of Information & Communication</td><td colspan="4">• "Act on the Protection of Information and Communications Infrastructure": Protection of Information in public/financial/IC sectors. Information Communications Infrastructure Protection Committee</td></tr>
<tr><td>Response against Infringement</td><td colspan="2">• "National Cybersecurity Management Regulation": Response against infringement in the public sector, National cybersecurity center</td><td rowspan="3">"Act on Promotion of Information and Communication Network Use and Protection of Information"</td><td>• Response against infringement in the private sector
• Center for Response against infringement</td></tr>
<tr><td>Cybersecurity Policies and Initiatives</td><td rowspan="2">"Electronic Government Act"</td><td>• Establishment and implementation of cybersecurity policies such as communication network of information</td><td>• Information protection for users
• Prohibition on network infringement</td></tr>
<tr><td rowspan="2">Assessment, Authentication, and Examination</td><td>• Security of electronic document
• The Common Criteria Evaluation and Validation System in public sector</td><td>• Safety Inspections for Information Protection
• Information Security Management System Certification</td></tr>
<tr><td colspan="4">"Framework Act on National Informatization": information security system evaluation and validation system</td></tr>
<tr><td>Digital Signature</td><td colspan="2">"Electronic Government Act": Administration electronic signature</td><td colspan="2">"Digital Signature Act": official electronic signature</td></tr>
<tr><td rowspan="2">Personal Information Protection</td><td colspan="4">"Act on the Protection of Personal Information"</td></tr>
<tr><td colspan="2">• "Protection of Personal Information in a Public Institution"
• "Resident Registration Act"</td><td colspan="2">• "Act on Promotion of Information and Communication Network Use and Protection of Information"
• "Protection of Credit Information Act"</td></tr>
</table>

Source: Korea Communications Commission, 2011:12 cited in Lyu, et al. 2015:10

Table 1 indicates that there are many laws related to cybersecurity and a number of departments managing them, which has led to negative effects in establishing and implementing cybersecurity policies in a consistent and systematic manner. Particularly with regards to the policies of authentication, there have been challenges in cooperating with each other among agencies and implementing policies in a reliable way because of conflicting interests and the differing direction of policy for each agency. For instance, the Ministry of Government Administration and Home Affairs tends to consolidate security of cyberspace, while the Ministry of Science, ICT and Future Planning as well as the Financial Services Commission tend to mitigate related regulations to enhance usability. This situation could cause interagency conflicts and confusion to the public.

Meanwhile, there has been little budget allocated to cybersecurity. For example, the amount of budget the Ministry of Government Administration and Home Affairs allotted to personal information protection was 9.8 billion won in 2015, of which only 1.3 billion won was used for cybersecurity such as maintenance of Public i-PIN (Ministry of Government Administration and Home Affairs, 2015). Many specialists evaluated that this budget would be inadequate to meet the cost of upgrading i-PIN after spending personnel expenses.

In this milieu, this study attempted to cover all aspects of cybersecurity including the current legal arrangement, governance structure, and public finance, human resources and so on by taking a "holistic and integrated approach."

2. Research Design

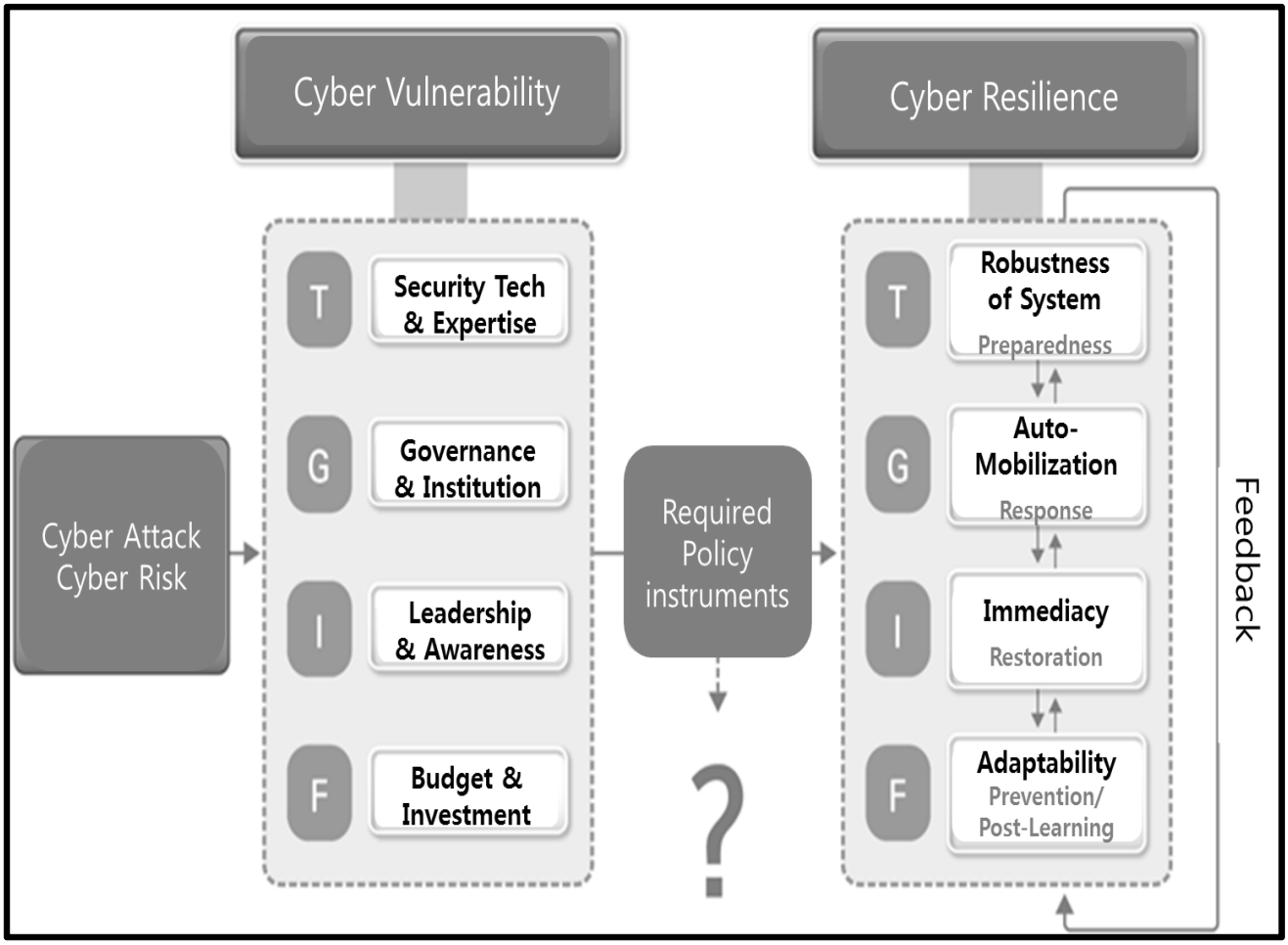
This study is divided into five steps; this study attempted 1) to explore different types of cyber threats and the current state of cyber breaches; 2) to examine the changing paradigm of authentication security systems and diversified authentication along with the advent of new technology; 3) to establish a theoretical framework, based upon the concept of resilience as well as vulnerability of cyberspace; 4) to examine domestic personal authentication technology, the pattern of usage by individuals and corporations, and budget, policies, and governance system related to authentication; 5) and to conduct an AHP (Analytic Hierarchy Process) survey in order to prioritize national cybersecurity policy.

More specifically, this study aspired to identify and compare the key cyber vulnerability and cyber resilient factors in both domestic and foreign cybersecurity environments. Based upon the "cyber resilience analytical framework" (see Figure 1), this study categorized cyber resilience into four dimensions; robustness, resourcefulness, rapidity, and adoptability. Then it further developed a new national cybersecurity, "TGIF." T (Technology) stands for technology & expertise, G (Governance) stands for governance and institution, I (Insights) stands for leadership and awareness, and finally F (Finance) stands for government budget for cybersecurity.

The key cyber vulnerability and resilience factors were drawn from the literature review, domestic and foreign case studies, and interviews with experts and practitioners in cybersecurity, and expert brainstorming. Then, an AHP (Analytic Hierarchy Process) survey was conducted so as to prioritize national cybersecurity policy.

In brief, through integrating findings from theoretical reviews, case studies, interviews and the AHP survey, specific policy implications and policy suggestions were drawn reflecting the aforementioned TGIF index.

Figure 1. Research model based on cyber resilience



Source: Lyu, et al. 2015:85

3. Domestic Cybersecurity Environment and Governance

3.1. Domestic Security Environment and Risk

Internet technology has developed rapidly in recent years. With the increase in mobile device usage changing the fundamental qualitative nature of Internet usage, data is being utilized in more ways than ever before. This trend is called "Technological Advancement and Convergence based on ICBM (Internet of Things, Cloud, Big Data, Mobile)," which has accelerated complexity, uncertainty, and risk in the cybersecurity environment (Friess, P., 2013: 9). In addition, ICBM frequently deals with a large amount of information and a majority of cybersecurity incidents typically occur due to personal information disclosure. The cybersecurity incidents could be categorized according to various fields of internet usage.

Table 2. Cybersecurity incidents in various fields

	Details
Privacy	(CCTV) CCTV made by Trendnet, a security camera company, could be tapped easily. In fact, about 700 videos recorded by the company's cameras were leaked.
	(Smart TV) Cameras in smart TVs were hacked in LA on August 2013.
	(Google Glass) Through Google Glass, people could collect personal information regardless of place or time; it was proved that the PIN number of bank account could be disclosed.
Smart Home	(Smart Home) Poofpoint, a security corporation in U.S., made public cases of cybercrimes that a hacker sent about 750,000 spoof emails by utilizing routers of home networks, smart TVs, and refrigerators.
	(Robot cleaner) Black Pearl Security gave a trial performance in terms of possibility that the camera embedded in a robot cleaner could be hacked and monitored in real time at ISEC 2014, Seoul.
	(Temperature controller) In the Black Hat USA 2014, a team from Florida demonstrated a temperature controller in the house could be controlled by a hacker.
	(Printer) At 44Con, an information security conference held in London on September 2015, showed that the Doom, which is a PC game, could be hacked through the LED screen of the printer. This indicates that any document in print requests could be stolen by hacking the printer.
	(Hotel) In the Black Hat USA 2014, a blinder, temperature, TV on-off, etc. of a hotel in China were controlled remotely through an IPad Ⅱ based on KNX protocol.
Network	(Car network) A hacker team from Spain made public circuit boards (20 dollars) which could invade car networks. This circuit board can approach the Control Area Network (CAN) which are installed in order for car corporations to check the system of computers in the car.
	(Home network) Kaspersky, a security corporation, reported that it invaded the home network through the home DSL router and spent less than 20 minutes in searching 14 weak spots.
	(Line Sharer) Team Cymru, a security consulting company, warned that about 300,000 line sharers made by D-Link, Tenda, Micronet, TP-Link, etc., were hacked.
Control System	(Industrial Control System) The United States Department of Homeland Security warned that the industrial control system which could be targets by hackers, because it has an internet connection without using firewall or authentication access control.
	(Air Control System) Korea Internet and Security Agency announced that the set-top box used for controlling air-conditional systems was abused through DDos attacks in Korea.
Medical Service	(Insulin pump) It was proved at the Black Hat Security conference in 2012 that an insulin pump could be manipulated by a hacker away from 800m and inject a fatal dose of insulin.
Transportation	IOActive Labs, a security company, inspected remote sensing technique of cars made by Sensys Networks. As a result of investigation, it found defects in the aspects of design and security, which meant a hacker could transmit fake data to the traffic management system and control the infrastructure such as traffic lights.
Cyber Crime	Europol asked the government to suggest countermeasures in order to respond to cybercrimes involving cars, medical equipment, wearable devices, other IoTs, etc.
	IID, a security corporation in U.S., projected that there could be cyber murder incidents using IoT technology in a few years. In fact, it is known that there might be a black market where people transact information with regard to security vulnerability of IoT equipment.
Broadcasting	(TVshing) The Black Hat USA made public the TVshing using 'Man In The Middle (MITM) in 2013.

Source: Institute for Information & Communications Technology Promotion (IITP), 2014:19 cited in Lyu et al (2015: 96)

3.2. Domestic Authentication Policy and Digital Governance

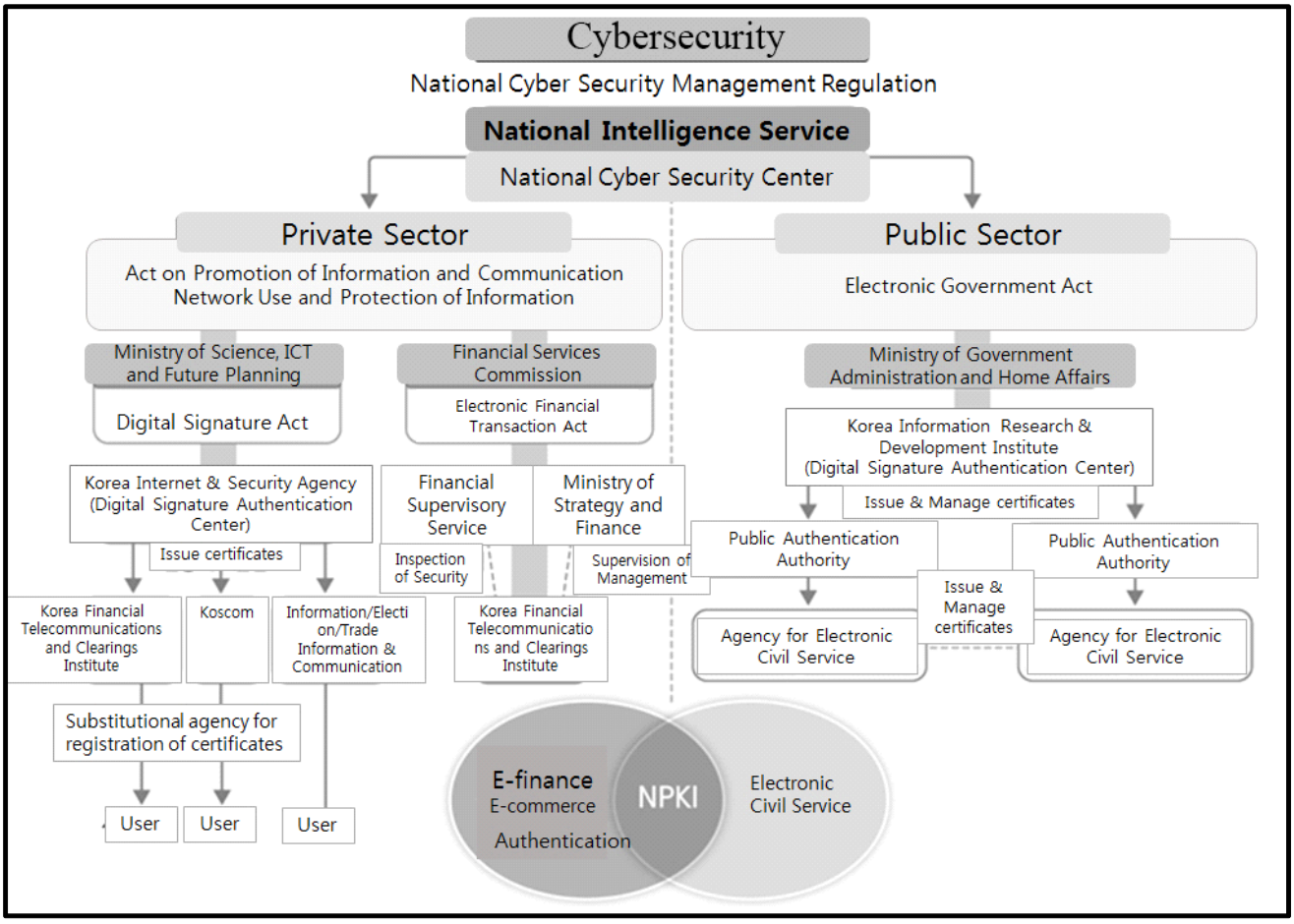
Various government departments, such as the Ministry of Government Administration and Home Affairs, Korea Communications Commission, the Ministry of Science, ICT and Future Planning, Financial Services Commission, etc., are being charged with tasks related to personal information protection. Each department has its own mandates, manpower, and organizational instruments, based on several laws and regulations. In the alternative, the central government announced the "Policy for Normalizing Personal Information Protection," which organizes the related laws and systems which extend across the agencies involved, through the "National Council for Policy Coordination" since 2014. Yet, there still exist issues pertaining to decentralized works of personal information.

Table 3. Mandates of agencies related to authentication

Ministry of Science, ICT and Future Planning	Korea Internet and Security Agency	Korea Financial Telecommunications and Clearings Institute
• Management and operation of "Public Key Infrastructure (PKI)" • Establishing policies for operating the PKI in a safe and reliable way. • Appointing authentication authorities, inspection, and request of correction order, work suspension, and cancellation of appointment • Implementing supervision of Korea Internet and Security Agency and authentication authorities based on laws and regulations related to the PKI • Conducting mutual agreement regarding the PKI with foreign governments	• Implementation of mandates grounded on the Article 25 of Digital Signature Act • Supporting examination of candidates for authentication authorities, according to the Article 4. • Supporting inspection of the authentication authorities, based on the Article 14-1. • Supporting evaluation and technology, based on the Article 18-3. • Implementing inspection of facilities and equipment for operation and management, according to the Article 19-2. • Working on various authentication tasks such as issuing and managing certificates • Conducting research in terms of developing technology and standardization pertaining to digital signature. • Supporting international cooperation such as mutual recognition and conducting research including system of digital signature. • Taking over members or certificates from authorities which are abolished or cancelled • Forwarding cases of the loss of authentication certificates to the authorities • Other duties in terms of digital signature	• Implementation of mandates according to the Article 4 and the Article 8 of Digital Signature Act • Accepting and processing application of authentication certificates • Verifying an enterer's identity • Issuing, reissuing, renewing, suspending, and abolishing authentication certificates. • Publishing information about authentication such as certificates and CRL • Operating substitutional agency for registration of certificates • Other duties required for the purpose of authentication authorities

Source: Homepage of each department (Ministry of Science, ICT and Future Planning <www.msip.go.kr>, Korea Internet and Security Agency <www.kisa.or.kr>, Korea Financial Telecommunications and Clearings Institute <www.kftc.or.kr>)

Figure 2. Governance for protection of information on cyber space



Source: Lyu, et al. 2015:133

The Table 3 and Figure 2 show that the Korean authentication system is a dual system, which is divided into both the private sector and the public sector. The private authentication system includes e-commerce and electronic financial transactions, while the public authentication includes e-government civil affairs. In this dual system, it is often pointed out that there might be a loophole or a blind spot regarding authentication, caused by having different agencies that supervise their own system security in different ways (Jung, 2013:30). Therefore, the current status of governance for protecting information on cyber space implies that an integrated system, which could manage and supervise personal information security such as management of I-PIN, is required.

4. Vulnerability and Resilience of Cybersecurity and Authentication

The vulnerability factors of cybersecurity were frequently found in domestic environment, compared with those of foreign environment, in various aspects of technology, institution, leadership, and perception (Von Solms, R., & Van Niekerk, J., 2013: 100). The most significant difference is to change the perception of public officials in terms of

cybersecurity. This is attributed to the fact that the change of perception and leadership could be followed by secondary factors such as standardization and advancement of technology, increased budgets, improved professionality of manpower, and other policy instruments.

Most vulnerability factors have an influence on resilience factors of cybersecurity. These two factors could be divided into two areas; technical and political. To begin with, vulnerability factors of cybersecurity are involved with technology, such as prevention-centered, under-developed, and isolated technology. It might have a positive effect on addressing these issues to adopt international standards of cybersecurity and apply technology in diversified ways including prevention, transaction, and post-response. In the political area, the vulnerability factors might be alleviated by reorganizing the system in order to secure enough budget and manpower as well as reduce redundant costs and time.

Table 4. Vulnerability and resilience factors of cybersecurity

	Vulnerability Factor	Resilience Factor
Domestic Environment	• Prevention-centered technology • Outdated security technology • Unorganized system of management (lack of governance and/or decentralized security system) • Different ways of authentication • Lack of budget • Lack of professional manpower • Insufficient regulations and laws regarding violations and crimes related to authentication • Unstandardized and isolated security technology • Low level of awareness about the importance of cybersecurity (especially in upper management)	• Application of new technology for prevention, exploration, and resilience • Training and acquisition of professional security personnel • Clarifying accountability and mandates across related agencies • Improving the status of office in charge of cybersecurity • International cooperation • Quantification of investment, such as cost-benefit analysis • Balanced budgeting for pre- and post-response • Enhancing multi-layer verification of identity (telephone, mail, message) • Reinforcement of security • Enhancing usability of authentication • Securing a sufficient budget • Introduction and adoption of standardized technology • Increasing awareness of public officers about cybersecurity
Foreign Environment	• Reluctance towards budgeting and investment because of uncertainty of cybercrime occurrence • Low understanding of information and communication compared to domestic environment • Low level of awareness by the public about cybersecurity • Less responsibility of public agencies with regard to cyber breach, compared with that of private organization • Little interest in the public sector	• Establishing a security framework with aims such as reducing crime rates, enhancing resilience, protecting interests, making cyberspace safe, and constructing knowledge (UK) • Proactive international cooperation (UK) • Repeated testing of resilience (UK)

Source: Lyu, et, al. 2015:182～183

In addition, with regards to the technical aspect, application of new technology and international cooperation are the key resilience factors of cybersecurity. With regards to the political aspect, it is important to clarify accountability and mandates among the various departments managing cybersecurity. Moreover, the perception of public officials about cybersecurity could be the vial factor for raising resilience, in that they might put more efforts in projecting cost and benefit analysis and allotting reasonable budget into cybersecurity (Shafqat, N., & Masood, A., 2016: 133).

Table 5. Vulnerability and resilience factors of authentication

	Vulnerability Factor	Resilience Factor
Domestic Environment	• Requiring excessive information • (After enforcement of ban on collecting resident registration numbers) Complex process of authentication (I-PIN, My-PIN) • Low awareness about the process of authentication • Low trust in the process of authentication • Complexity of the process of authentication • Only checks whether passwords are matching • Overreliance on website security systems • Mandatory certificate use • Multiple ways of authentication due to the advent of new technology • Insufficient investment for establishing security in electronic finance and payment • Possibility of replication without any permission • A single data terminal processing every step of authentication	• Application of international standardized cryptographic techniques • Development of mobile-based technology for authentication • Reinforcement of network security • Development of system reflecting user intent • Establishment of legislations and institutions regarding new authentication methods • Suggestion of binary or diversified steps of digital signature and governance of authentication • Simplification of authentication process • Increased investment in research about current vulnerability and development of alternative technology
Foreign Environment	• Inclusive definition of digital signature (EU, Germany) • Centralized operation of the authentication system (North Europe)	• Clarification of binary steps for digital signature to allow more flexible operation (EU) • Application of various ways for authentication (EU) • Expanding private autonomy, rather than government regulation (US) • Providing authentication by individual authorities, rather than by permission of the government (US) • Reducing usage areas of Social Security Numbers (US) • Inclusive and specific identification of digital signature (US) • Acceptance of both limited technical conditions and experimental technical conditions (German) • Autonomy of operation (UK) • Operation of accreditation systems rather than permission systems (Japan) • Introduction of voluntary authentication system (Japan) • Operation of actual examinations by organizations appointed as investigation agencies (Japan) • Minimizing risks by regulating frequency of exposing identification numbers (AU) • No designation of universal personal identification numbers (AU) • Acceptance of voluntary accreditation systems (Singapore)

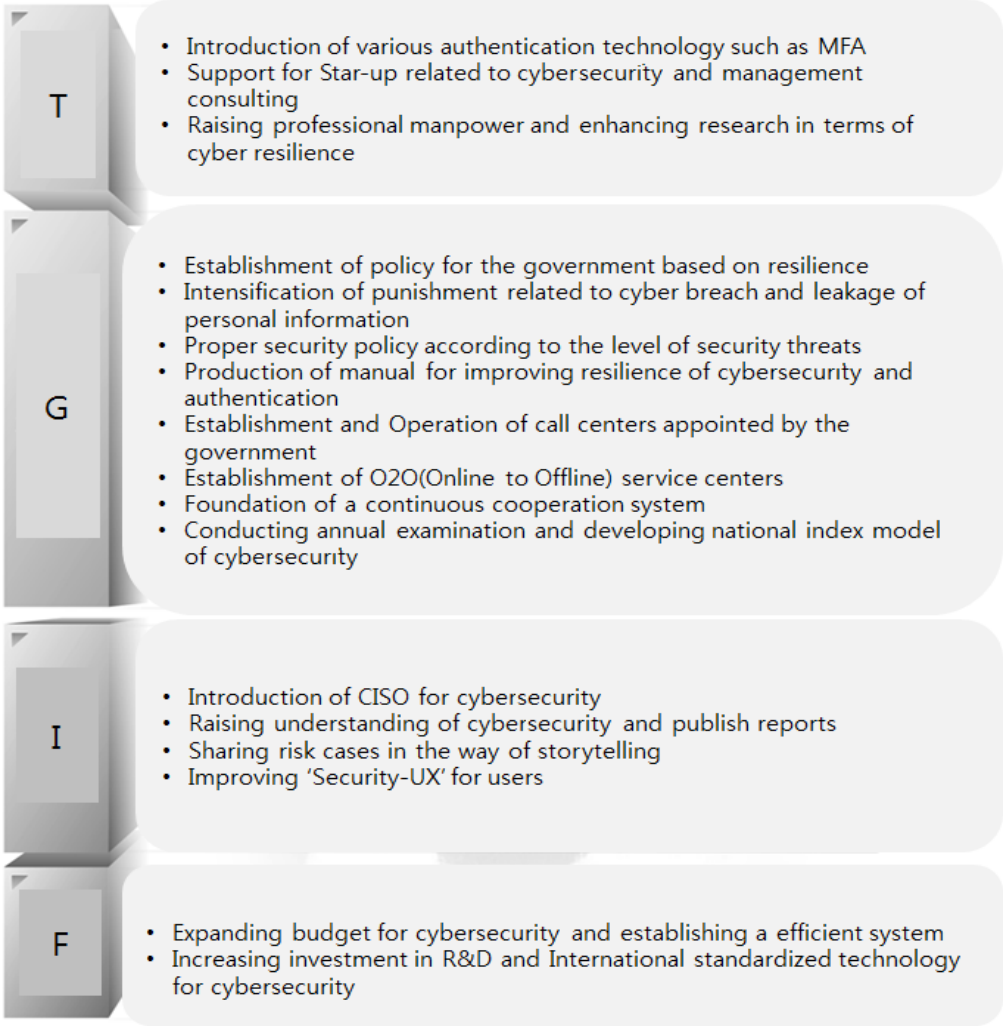
Source: Lyu, et al. 2015:182～183

The domestic environment related to authentication implies that the process of authentication is complicated and frequently requires users to send excessive information. The low level of trust in the process of authentication, a web-based authentication system, and a relatively low investment also were raised as vulnerability factors of authentication.

5. Policy Recommendation and Conclusion

This study conducted a policy workshop on both October 7th and 9th 2015, based upon the results of three iterations of the AHP survey, after drawing the key cyber vulnerability and resilience factors. A total of ten cybersecurity experts participated in this workshop so as to prioritize national cybersecurity policy in Korea. This study suggests new governance for improving resilience of cybersecurity. This governance is composed of four factors, technology, governance, insight, and finance (see below Figure 3).

Figure 3. New governance system for improvement of resilience



Source: Lyu, et al. 2015:271

In conclusion, this study suggests a number of policy implications for a better cybersecurity governance in Korea. First of all, the domestic cybersecurity system ought to be more enhanced by embedding high technology to predict and prevent cyber breach. Thus, the technology neutrality could be the key element for developing various technologies pertaining to security and authentication.

Secondly, the government should establish cooperative governance and an interchangeable system in order for the government to promote responsibility, to identify mandates, and to response various cybercrimes timely and efficiently.

Moreover, the government needs to recruit professional manpower to have expertise in terms of cybersecurity and to further raise awareness about it. It could have a positive influence on improving both the quality and quantity of policies related to cybersecurity to change the perception of chief administrators in the department. Job training and education also might be the key elements for changing the culture of organizations with regard to the importance of cybersecurity.

For the final point, budget is an important factor for the new governance system. The government should conduct strategic planning and establish integrating pre- and post-response by expanding budget related to the cybersecurity.

References

Fast IDentity Online (FIDO) Alliance. (2015). Federal Gov't Near 100% 2Factor Authentication, Retrieved from <https://goo.gl/F936TD.>

Financial Supervisory Service. (2014). Financial Supervisory Information. 2014-3:764.

Friess, P. (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.

Institute for Information & communications Technology Promotion (IITP). 2014. Current State of IoT and Major Issues. 2014:19.

Jung, Gi Seok. (2013). Study on improvement of authentication systems for electronic financial transactions. Convergence Security, 13(6), 25-33.

Korea Communications Commission. (2011). A Study on Solutions for the Advancement of Security Legislation.

Korea Communications Commission. (2014). Current State of Personal Information Leakage in 2010-2014.

Lyu, H.S. et, al. (2015). A Study on Cybersecurity Policy and Governance in the ICT Convergence Environment: Focused on "Authentification". KIPA Research Report 2015-24. Korea Institute of Public Administration.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. (2013, November). Privacy awareness about information leakage: Who knows what about me?. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (pp. 279-284). ACM.

Ministry of Government Administration and Home Affairs, 2015, Annual Budget Report FY2015.

Otto, P. N., Antón, A. I., & Baumer, D. L. (2007). The choice point dilemma: How data brokers should handle the privacy of personal information. IEEE Security & Privacy, 5(5).

Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cybersecurity Strategies. International Journal of Computer Science and Information Security, 14(1), 129.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. Computers & Security, 38, 97-102.