The Human Factor Of Cybersecurity And The Prevention And Counter Measures Against Cybercrime In South Korea

Sungha Park¹, Jungbin Lim², Dongkyu Kim³

¹School of Law, Seoul National University, Republic of Korea.

²Department of Psychology, Sungkyunkwan University, Republic of Korea.

³Master's program in Intellectual Property, Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea. Pritzker School of Law, Northwestern University, Illinois, United States of America.

ABSTRACT: The "National Cyber Security Strategy," established by the Republic of Korea Government in 2019 for the first time since its foundation, contains information on human and cultural factors of cybersecurity. This is to reflect the importance of human factors by breaking away from the convention that cyberattacks and security threats can be controlled only by technical means. The present study investigated the importance of human factors in cybersecurity and examines how the Korean government's cybersecurity policy deals with human factors. A survey on 274 participants revealed that there were ① differences in cybersecurity prevention behavior depending on individualistic-collectivistic values, ② the practice rate of preventive measures against cybercrime was higher for those who received security training than those who didn't, and ③ preventive measures and countermeasures against cybercrime were limited to certain methods. Accordingly, security measures and training from diverse perspectives are required to prevent cybercrimes targeting individuals and organizations.

KEYWORDS: Cybersecurity, Individualism-Collectivism, Human Factors, Cybercrime Prevention, Cybercrime Response, Korean National Cyber Security Strategy, National Intelligence Service Korea

ACKNOWLEDGEMENTS: This research paper won the Excellence Award from the Cyber Security Research Paper Contest (Policy Section) hosted by National Intelligence Service Korea in 2021.

1. Introduction
The entry into an offline virtual society introduced by the coronavirus, coincident with the rising importance of cybersecurity vastly changed the overall lives of our society (Korea National Intelligence Agency et al., 2021). After the outbreak of the coronavirus pandemic, cybercrime has increased by 48% in 2020 compared with the previous year (KBS News, 2021). In addition, through
a private cyber crisis response training held by the Korea Internet & Security Agency (KISA) in June 2019, the infections rates from malicious codes has increased 5 times compared to the first half of 2018 (Yonhap News Agency, 2019). The National Intelligence Service (NIS) underscored that approximately 40,000 domestic smartphones were hacked via hacking applications impersonating financial institutions, and that every individuals’ efforts are required for personal cybersecurity (Aju News, 2021). As an offline virtual environment becomes more common, cyberattacks targeting smartphones and personal computers are ought to increase, emphasizing the importance of cybersecurity more than ever before.

Similarly, our society confronts serious challenges due to cybercrime and various unethical behaviors aroused by the dysfunction of transition into an information-oriented society. Cybercrime can be understood as a concept of crimes in the real life moving into the cyberspace domain through expansion of time and space caused by the spread of computers and mobile terminals. According to police statistics from the National Police Agency, cybercrimes are increasing every year from 144,679 cases in 2015, 153,075 cases in 2016, 131,734 cases in 2017, 180,499 cases in 2019, and 234,098 cases in 2020 (Korean National Police Agency, 2022b). Considering that these figures are only from disclosed data identified by the National Police Agency, it can be assumed that actual cybersecurity damage ought to be more.

The Korean government is striving to prevent cybercrime. To this end, the Korean government established and published the "National Cyber Security Strategy" in April 2019. According to the publication, the Korean government aimed to promote and integrate 18 key tasks and 100 detailed tasks step-by-step until 2022. In addition, the Korean government is coordinating national cybersecurity policies and actively sharing threat information by strengthening cooperation systems between government branches in order to strengthen and synchronize domestic cooperation in national cybersecurity (Ministry of Science and ICT, 2019). Recently, the NIS began sharing cyber threats related information with private companies, surpassing previous precedents limited to intra-governmental cooperation. For instance, the NIS provides related information to 290 public institutions and 14 defense companies, that are targets with high possibility of hacking with key technologies after the coronavirus outbreak, i.e. pharmaceutical and bio industries, telecommunications, and information protection, etc. (The Science Times, 2021).

Among the diverse factors of cybercrime, a special emphasis on the “human factor” has been drawing attention. The proponents of the importance of human factor in cybercrime regards cultural factors, composed of human psychological factors, as a major cause of cybercrime, beyond institutional or technological factors. Consequently, the need for research on human psychology and its relevance with cybercrime has been raised, establishing academic forums studying the “psychology of those being hacked.” These studies suggest human factors or philosophical and cognitive approaches as alternatives to technical approaches to preventing cybercrime damage (K. Lee, 2008). The main purpose of these studies is to cultivate the notion on "human behavioral science, social psychology, organizational psychology, etc. in security issues" (The Asia Economy, 2021).

To this end, the present study examines the human factors of cybersecurity and how the Korean government's policy addresses these issues. We hypothesized that collectivistic-individualistic value orientation will affect participants' cybersecurity awareness and implementation of individual preventive measures. Also, we analyzed the effects of security training completion on the practice rate of preventive measures and countermeasures against cybercrime, and then discussed implications on Korea’s national cyber policy.
2. Cybersecurity and Human

2.1. Cybersecurity and Human Factors
Recently, cybercrime has been vastly increasing, bringing about ranging damage to companies and the public. Furthermore, the scale and degree of cybercrime damage have expanded due to its expanded range and intervention by states and even terrorist organizations, transforming into a threat posed against national security (The Office of National Security & the Blue House, 2019). Cybercrime is composed of several factors, such as ①technical factors, i.e. the vulnerability and risk of mediums caused by non-face-to-face, anonymous, and reproducible characteristics ②human factors, i.e. user’s attitude in cyberspace, subjective norms, behavioral control, and demographic variables ③social systematic factors, i.e. laws and systems that promote the development of information protection technology and ④cultural factors, i.e. Internet users' maturity of thoughts and cyber ethical matters on cybersecurity issues (K. Lee, 2008). As such, it is suggested that for the successful execution of cybersecurity policies, research in conjunction with adjacent disciplines in various fields should be conducted, beyond just technical factors (or perspectives) (P. Choi, 2021).

Among the factors listed above, this paper examines the human factors of cybersecurity. The cyber domain is where individual technical competence or knowledge is considered an important asset due to its state-of-art characteristics. Therefore, an individual's maturity and knowledge against cybercrimes such as spams, cyber sexual harassment cyber defamation, virus and hacking damage, data leakage and financial damage are of special importance (K. Lee, 2008). Therefore, the outdated notion that cyberattacks and infringements can be prevented and controlled only via technical countermeasures must be modified, and the need for human intelligence (HUMINT) and capability improvement is crucial in the cyber security domain (Chung & Lim, 2014).

These human factors constitute a cyber-culture, where they are illustrated through the user’s awareness of cyber safety and cyber ethics. In particular, cybersecurity needs to be alerted in that once it collapses, it can cause "significant social losses as well as economic losses due to the serial loss of trust in cyberspace." This shows the necessity for cyber ethics training, which entails the responsibilities and norms that users must bear in cyberspace (K. Lee, 2008).

2.2. Government’s Cybersecurity Policy and Human Factors
Introducing the concept of complex geopolitics, Kim explains that if the threat to emerging security such as cybersecurity is overlooked, the security threat will have spill-over effects and transfer to the traditional security field (S. Kim et al., 2017). Furthermore, "hacking, which previously was nothing more than jokes made by hackers, has recently expanded to a cyber-warfare between countries", explaining that cybersecurity is a point where emerging security and traditional security meet, or collapse (S. Kim et al., 2017). For example, the United States government stressed that Huawei's issue is not only an industrial problem but also a security problem.

For the first time, in 2019, the Korean government published the official "National Cybersecurity Strategy" to protect the daily lives of the people and the economic activities of companies threatened by soaring cybercrime and terrorism. In particular, the preface of the document states that "the safety of cyberspace can be secured when the government, businesses, and individuals cooperate together" and the center of cybersecurity is on the people (The Office of National Security & the Blue House, 2019). Composed of six strategic tasks, this publication puts special emphasis on the human aspect, which is addressed in Main Task 5 "Creating a Secure Cyber Culture." Developing and distributing
core and basic cybersecurity regulations so that people can recognize the importance of cybersecurity and readily implement them in their daily lives are the focal points of the chapter. The detailed tasks under Main Task 5 are to ① develop and disseminate basic cybersecurity regulations so that the public can perceive the importance of cybersecurity and easily practice it in their daily lives ② develop and implement tailored cyber ethics and security education programs for respective aspects within the society, i.e. students, public officials, soldiers, and entrepreneurs ③ strengthen social responsibility to protect the cyberspace under the jurisdiction of companies and maintain the appropriate level of security for products and services (The Office of National Security & the Blue House, 2019).

Concretely, the Korean government executes cybersecurity functions through state agencies with expertise in accordance with its respective and independent area of responsibility and functions. According to the National Cyber Safety Management Regulations, the National Intelligence Service is responsible for general control and coordination of national cybersecurity policies to establish and implement national cybersecurity policies. In addition, the Ministry of Science and ICT is enhancing cybersecurity in the private sector, developing industrial cybersecurity, and strengthening cybersecurity capabilities. The Ministry of National Defense also strengthens defense functions related to cybersecurity, while the National Police Agency strengthens cybercrime prevention and investigation functions. The Financial Services Commission establishes electronic financial security policies and user protection and the Ministry of Health and Welfare also carries out medical security functions. The Ministry of Trade, Industry and Energy executes industrial security in the cyber domain (Joo et al., 2018). In addition, the Korean government recently enacted the ‘Cyber Security Task Regulations’ on December 31, 2020 to cope with matters necessary for collecting, writing, distributing information related to cybersecurity to prevent and respond against cyberattacks and threats. Article 10 of the regulation stipulates that cyber training must be conducted to improve the job competency of public officials, executives and employees who perform preventive and response tasks against cyberattacks and threats. This shows that the development and improvement of human cyber capabilities through cybersecurity education training is a part of the Korean government’s cybersecurity policy.

3. Research Method and Design

3.1. Participants
Two hundred and seventy-four Koreans aged 19 and above participated in an online questionnaire. The demographic composition of the participants is presented in Table 1.
Table 1. Demographic Composition of Participants

| Sum | 198 | 70 | 2 | 274 |

3.2. Measures

3.2.1. Individualistic-Collectivistic Value Orientation
Individualistic-collectivistic value orientation refers to two contrasting worldviews regarding the nature of the relationship between the individual and the group (Hofstede, 1980). People with individualistic value orientation value prioritize individual goals and interests, while people with collectivistic value orientation prioritize group interests. Individualistic-collectivistic value orientation is a constituent concept applied to various social behaviors. Therefore, we expected that individualistic-collectivistic value orientation will affect people’s perception of cybersecurity and preventive measures against cybercrime.

Individualism-collective value orientation was measured through a reconstructed eight-item questionnaire widely used in previous studies (H.-S. Choi et al., 2018). Conflicting sentences representing 'collective value orientation' and 'individualism value orientation' were presented on each side of the questionnaire respectively, and participants indicated the extent to which they agree with either of the two sentences (6-point scale). The questionnaire consisted of four questions measuring 'group-person goal priority' and four questions measuring 'cooperative-competitive behavior patterns'. If the average score of the responses to the eight questions exceeds 3.5, the participant was categorized as a collectivist, and if less than 3.5, the participant was categorized as an individualist.

3.2.2. Preventive Measures against Cybercrime Damage
The practice rate of preventive measures against cybercrime was measured by questions widely used in previous studies (Korean National Police Agency, 2022a); In addition, participants responded to questions asking whether they have received security training from their institutions.

3.2.3. Experience and Countermeasures against Cybercrime Damages
Cybercrime damage experience involving network use and network infringement was measured, based on the classification of cybercrime by the National Police Agency; Cyber fraud (direct transaction fraud, shopping mall fraud, game account fraud, etc.), cyber financial crime (phishing, pharming, smishing, memory hacking), personal and location information infringement, cyber copyright infringement, and/or browsing. Subsequently, participants who responded that they experienced cybercrime damage were measured whether or not they implemented countermeasures after the damage. Questions were measured on a 7-point scale.

4. Results of the study

4.1. Collectivism-Individualism Value Orientation and Preventive Measures against Cybercrime Damage
In order to find out the effect of collectivism-individualism value orientation on preventive measures against cybercrime damage, a t-test was conducted to analyze whether differences in preventive measures according to collectivism-individualism value orientation was statistically significant. The
results show a statistically significant difference in the degree of preventive measures against cybercrime damage of people with collectivistic value orientation and individualistic value orientation (p=0.04). Analysis results are presented in Table 2.

<table>
<thead>
<tr>
<th>M</th>
<th>SD</th>
<th>t-value</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Practice Rate of Preventive Measures against Cybercrime</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collectivist (n=174)</td>
<td>Individualist (n=100)</td>
<td>Collectivist (n=174)</td>
<td>Individualist (n=100)</td>
</tr>
<tr>
<td>4.53</td>
<td>4.18</td>
<td>0.97</td>
<td>0.99</td>
</tr>
</tbody>
</table>

**Table 2. T-test result**

In order to find out the effect of collectivism-individualism value orientation and cybercrime damage experience on the practice of preventive measures against cybercrime damage, a two-way ANOVA was conducted. The result shows that people with individualistic value orientation showed a higher practice rate of preventive measures against cybercrime damage when they had experienced cybercrime damage than those with no experience, but the difference was not statistically significant. Analysis results are presented in Table 3.

<table>
<thead>
<tr>
<th>SS</th>
<th>df</th>
<th>MS</th>
<th>F-value</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value Orientation (A)</strong></td>
<td>0.92</td>
<td>1</td>
<td>0.91</td>
<td>0.94</td>
</tr>
<tr>
<td><strong>Cybercrime Damage Experience (B)</strong></td>
<td>0.29</td>
<td>1</td>
<td>0.29</td>
<td>0.30</td>
</tr>
<tr>
<td><strong>AxB</strong></td>
<td>2.07</td>
<td>1</td>
<td>2.07</td>
<td>2.13</td>
</tr>
</tbody>
</table>

**Table 3. ANOVA result**

A t-test was conducted to find out the effect of security training completion on the practice of preventive measures against cybercrime. The results show a statistically significant difference in the degree of practicing preventive measures against cybercrime damage between those who completed security education and those who didn’t (p=0.01). Analysis results are presented in Table 4.

<table>
<thead>
<tr>
<th>M</th>
<th>SD</th>
<th>t-value</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Completed Training (n=162)</strong></td>
<td><strong>Did Not Receive Training (n=112)</strong></td>
<td><strong>Completed Training (n=162)</strong></td>
<td><strong>Did Not Receive Training (n=112)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4. T-test results

For a more detailed analysis, the security training completion rate for each industry was analyzed. The security training completion rate was in the order of large corporations (92%), military and public officials (76.67%), small and medium-sized companies (73.53%), and self-employed and start-ups (25%). Analysis results are presented in Table 5.

Table 5. Security Training Completion Descriptive Statistics

4.3. Countermeasures after cybercrime damage
Descriptive statistical analysis for each variable was conducted to find out the frequency of cybercrime damage experience and the practice rate of countermeasures and further preventive measures after the damage. First, the overall experience rate of crimes involving infringement of networks (56.20%) was higher than that of crimes involving usage of networks (32.12%). The overall analysis results are presented in Table 6.
Table 6. Cybercrime Damage Experience Descriptive Statistics

For countermeasures following cybercrime damage, the practice rate of changing all account passwords (49.41%) and learning personal information damage response procedures (43.53%) was relatively high, but the practice rate of reporting to the police and other related agencies (16.47%) was low. Analysis results are presented in Table 7.

Table 7. Countermeasures against Cybercrime Descriptive Statistics

For further preventive measures, the practice rate of reading personal information processing policy and terms of use (M=2.91), periodic password changes (M=3.30), awareness of name theft confirmation service (M=3.16), and awareness of personal information infringement report (M=3.32) was low. Analysis results are presented in Table 8.

Table 8. Further Preventive Measures Against Cybercrime Descriptive Statistics
I actively utilize reports of personal information infringement.

<table>
<thead>
<tr>
<th>Description</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collectivism-Individualism Value Orientation and Preventive Measures Against Cybercrime</td>
<td>Participants with collectivistic value orientation showed a higher practice rate of preventive measures against cybercrime than those with individualistic value orientation.</td>
</tr>
<tr>
<td>Collectivistic-Individualistic Value Orientation, Cybercrime Damage Experience, and Preventive Measures Against Cybercrime</td>
<td>Participants with individualistic value orientation showed a higher practice rate of preventive measures against cybercrime when they had experienced cybercrime damage than those who had not.</td>
</tr>
<tr>
<td>Security Training Completion and Preventive Measures Against Cybercrime</td>
<td>The practice rate of preventive measures against cybercrime is higher for participants who have completed security education than those who have not.</td>
</tr>
<tr>
<td>Descriptive Statistics for Completion of Security Training</td>
<td>Completion rates are in the order of large corporations, military and public service, small and medium-sized enterprises, and self-employed and startups.</td>
</tr>
<tr>
<td>Post-damage countermeasures and further preventive measures</td>
<td>Practice rate of changing passwords and leaning damage response rules are high, but rate of reporting to the police and the utilization of institutions such as the Personal Information Infringement Protection Center is low.</td>
</tr>
</tbody>
</table>

**Table 8. Further Preventive Measures against Cybercrime Descriptive Statistics**

**5. Discussion**

Overall, the present study was meaningful in terms of analyzing the effects of collectivistic-individualistic value orientation and cybercrime damage experience on preventive measures and countermeasures against cybercrime damage. The main results are summarized and presented in Table 9.

<table>
<thead>
<tr>
<th>Description</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>① Collectivism-Individualism Value Orientation and Preventive Measures Against Cybercrime</td>
<td>Participants with collectivistic value orientation showed a higher practice rate of preventive measures against cybercrime than those with individualistic value orientation.</td>
</tr>
<tr>
<td>② Collectivistic-Individualistic Value Orientation, Cybercrime Damage Experience, and Preventive Measures Against Cybercrime</td>
<td>Participants with individualistic value orientation showed a higher practice rate of preventive measures against cybercrime when they had experienced cybercrime damage than those who had not.</td>
</tr>
<tr>
<td>③ Security Training Completion and Preventive Measures Against Cybercrime</td>
<td>The practice rate of preventive measures against cybercrime is higher for participants who have completed security education than those who have not.</td>
</tr>
<tr>
<td>④ Descriptive Statistics for Completion of Security Training</td>
<td>Completion rates are in the order of large corporations, military and public service, small and medium-sized enterprises, and self-employed and startups.</td>
</tr>
<tr>
<td>⑤ Post-damage countermeasures and further preventive measures</td>
<td>Practice rate of changing passwords and leaning damage response rules are high, but rate of reporting to the police and the utilization of institutions such as the Personal Information Infringement Protection Center is low.</td>
</tr>
</tbody>
</table>

**Table 9. Summary of main results**

**5.1. Value orientation and preventive measures against cybercrime**

The results indicate that those with high collectivism tendencies had a relatively higher practice rate of preventive measures against cybercrime damage than those with individualism value orientation. Furthermore, if individualistic tendencies were high, the practice rate for preventive measures against cybercrime damage was relatively low.

Collectivism, a concept in which groups are prioritized over individuals, emphasizes cooperation and harmony among group members. Korean collectivism shows an emphasis on forming good
relationships between oneself and group members (Yang, 2019). One successful case of collectivism in Korea is the COVID-19 quarantine process, where various media highlighted the advantages of Korean collectivism, with people showing strong unity in pursuit of collective interests (The Opinion News, 2021). As such, collectivism, which is often used with a negative connotation, can sometimes lead to desirable results. Similarly, this study shows the importance of promoting group awareness in terms of cybersecurity prevention. In particular, collectivism can have a positive effect on organizational performance by establishing institutional mechanisms for job involvement and organizational commitment (Maeng & Kim, 2019).

However, the results also indicate that people with individualistic tendencies have increased implementation of preventive measures only when they had experienced cybercrime damage. Nevertheless, cybersecurity is important not only for individuals but also for the security of companies and countries as it is linked to the leakage of technologies that are national or industrial secrets and corporate trade secrets. For this reason, looking at the mid- to short-term implementation plan of the 2011 U.S. cyberspace policy review, a pan-national awareness and education campaign to promote cybersecurity was designated as an implementation task (J. Lee & Yoon, 2012). Previously, the White House pointed to operations as one of the major causes of cybersecurity threats in 2003, and said that operations are generally related to enforcing security policies, responding to intrusions, and restoring major services. These operations are also done by humans, and it is necessary to have a sense of mission to see how important personal security consciousness is for the organization and community. Therefore, macro and micro efforts are required to inform individuals of the importance of preventing cybercrime damage, and the significance of protecting industrial security, trade secrets, and even national core technologies can be reflected in the mission statement.

5.2. Effects of security training on preventive measures against cybercrime
The results show that the practice rate of preventive measures against cybercrime was high among those who completed security training. As such, this indicates that security training may contribute to raising cybersecurity awareness.

However, the completion rate of security training differed depending on the type of industry. Participants' security training completion rate differed in the order of large corporations (92%), military and public service (76.67%), small and medium-sized companies (73.53%), and startups (25%). Since most workers receive security training through programs conducted by their employer, it could be inferred that there is a relationship between the type of industry and security training completion. In particular, startup employees showed noticeably low security training completion rates. The reason may be because smaller companies such as startups cannot readily offer security training due to budget shortages (The Economic Review, 2016). Therefore, while security education should be more active in all organizations, more efforts should be made to support startups with low security training completion rates.

Another notable result is that 73.53% of workers in small and medium-sized enterprises completed security training, which is comparable to the completion rate of military and public officials (76.67%). This shows that the security training completion rate of SMEs, which are relatively vulnerable in providing security training by its inherent nature, has increased following national-level efforts. The Ministry of SMEs and Startups and the Small and Medium Business and Agricultural Cooperation Foundation operate technology protection fences for SMEs in accordance with the Small and Medium Business Technology Protection Support Act. However, despite national support for SMEs and the
high security training completion rate of employees, the technology protection capabilities of SMEs still show a large difference compared to large corporations as shown in Table 10. In addition, another implication for cybersecurity training is that there were exceptionally many cases technical data leakages by e-mail and mobile devices in 2018. This shows that there is a need to improve the quality of security training for small and medium-sized enterprises.

Companies operate various training and development programs to improve job satisfaction as well as career development of individual employees. For example, on-the-job training, apprenticeship programs, off-the-job training, and online training are being conducted, which may include cybersecurity training (S. Kim et al., 2019). Most large companies train their employees through these training programs, but small companies are known to conduct such programs informally (S. Kim et al., 2019).

<table>
<thead>
<tr>
<th>Year</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large Corporation</td>
<td>67.2</td>
<td>67.9</td>
<td>70.3</td>
<td>69.3</td>
</tr>
<tr>
<td>Middle-Market</td>
<td>59.4</td>
<td>60.3</td>
<td>60.9</td>
<td>66.8</td>
</tr>
<tr>
<td>SMEs</td>
<td>49.3</td>
<td>51.3</td>
<td>44.9</td>
<td>47.5</td>
</tr>
</tbody>
</table>

Table 10. Technology Protection Capability Comparison Chart

However, according to a study on the effectiveness of security training, education on spam email was effective in lowering the actual email access rate, but this effect did not last more than three months (B. Kim et al., 2018). In addition, there is criticism that general security awareness education and training was not effective in raising the responsibility and security awareness of trainees and reducing moral hazard (Shim, 2017). Therefore, it should be noted that the effect of education appears only when the efforts of the trainees are converted to a specific value (Shim, 2017).

There is a point that could be made from that fact that the practice rate was high in the order of large companies, startups, small and medium-sized enterprises, military and public officials. Technology-oriented startup workers may possess a high awareness of preventing cybercrime damage, but the relatively low awareness among military and public officials, who have access to national-level technology may potentially be a significant issue. To overcome this, local municipalities, including the government, are already making various efforts to prevent personal and security information leakage accidents, and it is necessary to develop a high level of security awareness by sharing cases of cyber infringement to public officials.

5.3. Further Prevention and Countermeasures
The results show that people generally make efforts to prevent cybercrime damage. In particular, the practice rate for using passwords that are difficult for others to infer, identify personal identification measured in place of resident registration numbers, not informing others of personal information, not storing personal information in a shared folders, and not downloading data from unknown sources were relatively high. However, the practice rate was high only in certain areas. On the other hand, the practice rate of carefully examining personal information processing policies and terms of use and periodically changing passwords was relatively low. However, the aforementioned items have
received criticism from experts regarding their preventive effect. The U.S. National Institute of Standards and Technology (NIST) removed the recommendation to set a password expiration date from the guidelines in the Digital Identity Guidelines published in June 2017 (Grassi et al., 2017). This is because the guidelines have made it easier for hackers to figure out the pattern of the password of an account by changing only a small portion of the password for most users (The Wall Street Journal, 2017). In Korea, studies have been conducted that setting a password expiration can increase the reuse rate of the same password, and for the same reason, the password selection and use guide published by the Korea Internet & Security Agency (KISA) enforces password change only "if exposed to a third party." Criticism has been raised over whether prior consent systems such as personal information processing policies and terms of use can sufficiently protect internet users' rights such as "personal information self-determination." The current method of prior consent in Korea is that the user becomes insensitive to consent by repeating meaningless consent procedures, and furthermore, even if the terms and conditions are unfair, the site operator is exempted as the user had consented seemingly (Jeon & Kwon, 2019). These criticisms are common in that the behavior patterns of the user differ from those intended by the relevant guidelines and institutions, resulting in substantial failure to protect the rights and interests of the user. Therefore, some preventive activity regulations should be improved in consideration of the security effects resulting from the actual behavior patterns caused by the regulations.

The result also showed differences in the implementation of countermeasures following cybercrime damage. The practice rate of changing password of all accounts, and the learning personal information infringement response procedures were relatively high (49.41% and 43.53% respectively). However, only 16.47% of participants reported to state agencies such as the police or the NIS, and 21.18% of participants asked their acquaintances for. In addition, even though hacking accounted for 51.76% of participants’ cybercrime damage experience, the practice rate of using the name theft confirmation service and the utilization of personal information infringement reports were notably low (M=3.16 and M=3.32 respectively). This indicates that even though there are sufficiently helpful specialized institutions in cybercrime response, the majority of those affected by cybercrime tend to solve the problem themselves rather than receiving help from state agencies or specialized institutions.

Recent cybercrime usually does not end with a one-time damage, as the leaked personal information may cause secondary damage through additional attacks such as phishing or hacking. Furthermore, APT attacks on companies and government agencies sometimes begin with attacks against individuals. Therefore, efforts are needed to actively promote policies with low public awareness, such as personal information infringement reports and name theft confirmation services, so that the scale of damage can be limited by identifying and responding to cybercrime damage early on.

6. Conclusion
In order to protect information, the Korean government holds an annual "Information Protection Day" ceremony, promoting awareness of cybersecurity among the public (Korea National Intelligence Agency et al., 2021). To this end, the government aims to develop human factors for cybersecurity as well as public relations of national policy. Beyond personal level of infringement, cyber infringement can also expand to leakage of state technology, industrial technology, and trade secrets of companies.

Cybercrime prevention measures can be categorized into technical factors, human factors, institutional factors, and cultural factors. The present study attempted to examine the relationship...
between cybersecurity and human factors. To this end, the Korean government’s first "national cybersecurity strategy" stipulates awareness of the importance of cybersecurity, dissemination of basic cybersecurity rules in daily life, development of implementation of customized cyber ethics and education programs, and promotion of corporate social responsibility to protect cybersecurity. In addition, the Ministry of Science and ICT and related organizations collaborate with the private sector, and the National Intelligence Service also plays a pivotal role in preventing cybercrime. Subsequently, a survey of 274 participants aged 19 or older with Korean nationality have shown the following results.

First, there was a difference in the implementation of preventive measures against cybercrime according to participants’ value orientation. People with collectivistic value orientation showed a higher practice rate of preventive measures against cybercrime than those with individualistic value orientation. On the other hand, individualistic participants increased implementation of preventive measures only when they suffered cybercrime damage. Cybersecurity can extend beyond individual problems to problems that involve the fate of a company or a country. Therefore, as stipulated in the national cybersecurity strategy, reflecting the importance of cybersecurity in corporate missions could be one way to strengthen the human factors of cybersecurity.

Second, those who completed security training had a high rate of implementing preventive measures against cybercrime. Most security training is conducted in the participants’ workplace, and the training completion rate was in the order of large companies, military and public service, SMEs, and startups. In addition, for preventive measures against cybercrime, the practice rate was in the order of large companies, startups, SMEs, and military and public service. These results suggests a potential issue that military and public officials dealing sensitive data on national policy have relatively low awareness of preventive measures against cybercrime. To this end, the Ministry of SMEs and Startups as well as various local governments are making efforts to prevent security breach accidents, and it is necessary to expand support for such training and also improve its quality. In particular, the National Police Agency specifically specifies preventive measures for each crime type, which should be actively utilized (Korea National Police Agency Cyber Bureau, 2022).

Third, practice rate of further cybercrime prevention and countermeasures were concentrated on only certain measures. The proportion of participants who experienced cybercrime damage was significantly high. Nevertheless, the practice rate of countermeasures following the damage was concentrated on only certain measures. After the damage, the practice rate of changing passwords of all accounts, and learning personal information damage response procedures were high, but the practice rate of reporting to related organizations such as the police and NIS remained low. The practice rate of using name confirmation theft services and the utilization of personal information infringement reports were also relatively low. Therefore, it is necessary to actively promote not only preventive measures but also countermeasures following cybercrime damage.

Recently, the types of cyberattacks are changing and diversifying more rapidly than in the past. In particular, cyberattacks are utilizing more advanced and intelligent methods, and the types of attacks are changing to a form that has a wider scope and purpose than the past (Jung & Chang, 2020). Therefore, it is required to establish security measures from a diversified perspective in order to secure the sustainability of cybersecurity of individuals and organizations.

References

Security.


The Asia Economy. (2021). We should also study the psychology of hacking.


The Science Times. (2021). Civil Entities, i.e. Security·Bio, Reviews Cyber Threat Information from NIS.


Yonhap News Agency. (2019). Malicious code infection rate of companies participating in cyber crisis response training is 5 times higher than last year.