Factors Affecting Corporate Security Policy Effectiveness in Telecommuting

Chulwon Lee and Kyungho Lee

1KB Financial Group Inc., 141 Uisadang-daero, Yeongdeungpo-gu, Seoul, Republic of Korea
2Korea University, Seoul, Republic of Korea

Correspondence should be addressed to Chulwon Lee; echulwon@gmail.com

Received 30 June 2021; Revised 4 August 2021; Accepted 25 August 2021; Published 8 September 2021

1. Introduction

1.1. The Increase of Telecommuting and Cyber Risk due to COVID-19. There has been a significant increase in teleworking practices in most companies worldwide after the COVID-19 pandemic. Only 29% of the waged and salaried employees in the United States could work from home in 2017 and 2018, that is, before the COVID-19 pandemic [1]. However, a Gartner survey of 317 CFOs on March 30, 2020, revealed that three-quarters of respondents plan to turn over at least 5% of their staff into teleworking permanently post-COVID-19 [2]. Baker [3] also said in July 2020 that 82% of CEOs also would map out a plan of relocating their staff to remote work.

Meanwhile, there was a 21% year-on-year increase in cyberattacks in the first quarter of 2020 itself [4]. In addition, according to the KISA (Korea Internet and Security Agency) survey report of May 2020, 51.57% of the 1623 respondents said that they had experienced hacking attempts and malicious code infections while telecommuting [4]. Also, the threat such as spear phishing employing malicious URLs is on the rise [5]. All systems of corporations connected to the Internet are vulnerable to cyberattacks (especially DDoS), and high value systems are more likely to be attacked owing to economic benefits [6]. Rubinstein [7] said that corporations need to take technical measures as well as expand their job training programs, to prevent potential hazards associated with telecommuting environments.

1.2. The Need for Research on New Environment. Several corporations have adopted relentless efforts to develop security policies and assorted control systems, as well as invested considerable time and money to secure their
primary assets from both external and internal threats. However, there are limited studies that help improve the effectiveness of information security policies in a well-controlled office space based on the theories of formal and informal control. It seems that the security controls according to these existing studies do not work exactly against the cyber threats that emerged in the COVID-19 pandemic.

According to D’Arcy et al. [8], an information security policy is the same as social rules. Therefore, just as social rules change according to the environment, the same is true for information security policies. Moreover, telecommuting security policies must be distinguished from existing security policies because the cyber threats during COVID-19 have not been previously observed in secure and well-controlled office spaces. That is why a new environment requires new controls.

To counter the unpredictable risks that have emerged during the volatile COVID-19 crisis, in this work, we propose a model based on social control theory, formal control, and general deterrence theory. We collected data from 207 experienced employees working in different telecommuting environments. The survey data confirmed the importance of specification and mandatoriness of policies in developing an effective information security policy for corporations: specification is to describe clearly and definitely security policies and mandatoriness is the degree to which individuals comply with security policies. As it was important to specify well security policy in mandatoriness in previous research, we also tried to find out the relation with specification and mandatoriness in telecommuting.

2. Materials and Methods

2.1. Literature Review. Numerous studies have been conducted on the factors affecting the effectiveness or implementation of security policies. We have taken a careful note of these studies, which utilized social control theory, formal control, and general deterrence theory, and built upon them to upgrade the security level and prevent information security breach from unknown cyber threats such as hacking and cyberterrorism within an organization.

Social control theory proposes that the effectiveness of a security policy is influenced by the following four factors: attachment, involvement, belief, and commitment [9]. Attachment is the close relationship with others at work. Involvement is the time and energy that employees invest in company activities. Belief is the degree to which workers think that taking certain behaviors is morally correct. Commitment is the employee’s recognition of and devotion to one’s role in company. According to formal control and general deterrence, a fear of punishment induces criminal deterrence, which can serve as an important strategy in cybersecurity [10]. In general, it has been shown that strict security control and a fear of punishment encourage employees to abide by security policies. In particular, D’Arcy and Devaraj [11] suggest that employee awareness plays a critical role in security control.

Lemay et al. [12] said that recent research studies about information security were concentrating on stimulating protective behaviors in users of information technology. According to Hsu et al. [9], extrarole behaviors and social control (i.e., social bonds) are mandatory to optimize the security policies of an organization. Moreover, it is necessary to encourage employees to follow security policies [9, 13–16]. Given that there are numerous examples of conflicts among members of an organization concerning in-role behaviors in the lack of organizational extrarole behaviors, we agree in part that Hsu et al. [9] emphasize the necessity of extrarole behaviors and social control for an effective information security policy.

Social controls that induce the fear of punishment play a decisive role in reducing the chances of information leakage according to general deterrence theory [8]. Moreover, user awareness regarding security policies, security education, training, and awareness (SETA) programs, and computer monitoring is likely to decrease the misuse of information systems, and the severity of sanctions outweighs the certainty of sanctions [8]. In addition, security education programs that provide employees with more information on security have been shown to have a positive impact on the effectiveness of security policies [10]. The best policy for users is to be aware and take the necessary precautions to maximize the effectiveness of a security policy [17].

However, one of the studies found that formal control did not affect the effectiveness of security policies. For example, the survey conducted by Wiant [18] on 140 information system managers revealed that the strategic application of a security policy is independent of the volume of security incidents or the reduction in accident severity. Moreover, Lee et al. [10] found that security policies and security systems do not have any influence on computer misuse.

As shown in Table 1, the aforementioned studies mainly focused on the security concerns arising in a limited office environment with the aim of preventing illegal behaviors and implementing security policies. However, our study takes a different approach to determine how the COVID-19 pandemic changes the implementation of security policies under exceptional circumstances, such as telecommuting environments.

2.2. Research Model. As shown in Figure 1, the aim of our research model was to study the effects of both mandatoriness and extrarole behaviors on the effectiveness of telecommuting security policies. In addition, mandatoriness and extrarole behaviors were hypothesized to be influenced by formal control, formal sanction, and informal sanction.

In the following sections, we discuss the model constructs and the underlying hypotheses in detail.

2.2.1. Effect of Formal Control on Telecommuting Security Policies. Corporations tend to reinforce the desired security behaviors in their employees to achieve their security goals [13, 19, 20] by sending signals that make their employees feel obliged to implement the necessary controls. It has been
shown that specifying the desired behaviors and corresponding outcomes is crucial for the implementation of controls [13, 19–21]. A security policy is a proposition regarding how the employees of an organization should conduct themselves and what are the consequences of their behaviors. A well-designed security policy is the first step toward outlining the core employee behaviors necessary to achieve the desired outcomes and a clear direction to enforce these behaviors [13]. Therefore, we hypothesize the following:

H1a: security policy specification affects positively the perceived mandatoriness in telecommuting environments

H1b: security policy specification affects positively extrarole behaviors (e.g., helping and voice) in telecommuting environments

Recalling the old saying in business, "Measurement leads to improvement," simply establishing policies and posting on office bulletin boards are not sufficient to effectively enforce the desired behaviors in employees [13, 22, 23]. Monitoring is a useful method that confirms the observance of security policies and is a way for the management to make their presence felt [13, 24]. It also provides a means to surveil the employee system logs. Moreover, if there is no compliance monitoring, then the employees tend to overlook the security policies. Therefore, monitoring has a positive ripple effect on employee awareness and it conveys the importance of security policy compliance as well. On this basis, we hypothesized the following:

H2a: monitoring security policy compliance affects positively the perceived mandatoriness in telecommuting environments

H2b: monitoring security policy compliance affects positively extrarole behaviors in telecommuting environments

It is natural that employees expect a reward for observing corporate security policies [13, 25]. Rewards, along with policy specification and compliance monitoring, encourage employees to conform to the security policies as well as to reinforce their behaviors [13, 26]. In short, when there is no reward for complying with the regulations, there is no motivation for the employees to continue to do so. Therefore, we hypothesized the following:

H6a: reward affects positively the perceived mandatoriness in telecommuting environments

H6b: reward affects positively extrarole behaviors in telecommuting environments

Table 1: Factors’ comparison.

| Factors | Factors |
|---------|---------|
| Hsu et al. [9] | Social control and extrarole behaviors |
| D’Arcy and Devaraj [11] | Certainty and severity of sanctions |
| D’Arcy et al. [8] | Severity of sanctions, SETA, and computer monitoring |
| Lee et al. [10] | Induction control intention, involvement, and belief |

Figure 1: Research model.
H3a: rewards for security policy compliance affect positively the perceived mandatoriness in telecommuting environments

H3b: rewards for security policy compliance affect positively extrarole behaviors (e.g., helping and voice) in telecommuting environments

2.2.2. Effect of Formal Sanctions on Telecommuting Security Policies. The underlying concept of deterrence theory is that the threat of punishment will deter corporate members from engaging in illegal behavior. In an organization, punishment and disciplinary action against employees are the main tools to keep the corporate ship afloat [11, 27]. Several studies on perceived-deterrence theory have shown that the severity and gravity of the imposed sanctions increase the effectivity of security policies [11, 27, 28]. Our study examined the levels of association in the effects of sanctions and security policies under telecommuting environments. Based on the preceding discussion, we hypothesized the following:

H4a: severity of formal sanctions affects positively the perceived mandatoriness in telecommuting environments

H4b: severity of formal sanctions affects positively extrarole behaviors in telecommuting environments

H5a: certainty of formal sanctions affects positively the perceived mandatoriness in telecommuting environments

H5b: certainty of formal sanctions affects positively extrarole behaviors in telecommuting environments

2.2.3. Effect of Informal Sanctions on Telecommuting Security Policies. Deterrence studies have shown that perceived criticism from friends, family, or work colleagues influences the decision-making behavior of employees [11, 28, 29]. From a deterrence perspective, informal sanctions have an effect similar to formal sanctions regarding the costs to be paid by the violator [11, 29]. Thus, we propose the following hypotheses:

H6a: moral beliefs affect positively the perceived mandatoriness in telecommuting environments

H6b: moral beliefs affect positively extrarole behaviors (e.g., helping and voice) in telecommuting environments

2.2.4. Effect of Mandatoriness and Extrarole Behaviors on Telecommuting Security Policies. The objective of security policies is to improve corporate security protocols. However, there is a gap between the individual understanding of security policies and the level of observance depending on the type of method used [13, 30]. One of the studies showed that only 60% of the employees in an organization adopted the Internet usage policy at face value and there exists a reasonable suspicion among employees regarding the significance of security policies [13, 22]. The most compelling force that encourages employees to comply with corporate security policies is management expectations [13, 31]. Hence, management expectations play a critical role in enhancing security policies in telecommuting. Therefore, we propose the following hypothesis:

H7: perceived mandatoriness affects positively the effectiveness of telecommuting security policies

Although most employees follow corporate security policies, it is likely that some would fail to comply with a specific set of security requirements owing to their poor security awareness, incompetence, irresponsibility, or low self-efficacy. Thus, it is important that employees help each other abide by corporate security policies; otherwise, the weak links in the organization could undermine the overall security policy [9]. Without the cooperation of employees, corporate security policies are far from reality [9, 15]. Moreover, chances are that the lack of engagement with extrarole behaviors could weaken the effectivity of security policies in telecommuting. It has been proposed that employees should be engaged in a positive manner to prevent each other from doing something wrong to enhance the effectivity of security policies. Therefore, we propose the following hypothesis:

H8: extrarole behaviors affect positively the effectiveness of telecommuting security policies

2.3. Research Methods

2.3.1. Study Design and Data Collection. Given the unprecedented global situation owing to the COVID-19 pandemic, distinct datasets from various organizations in Korea who encouraged their employees to telecommute were used to test our model. We conducted a survey with 207 employees who telecommuted during the pandemic. Table 2 provides the detailed demographic information of the respondents.

2.3.2. Constructs and Measurement. The effectiveness of telecommuting security policies during the COVID-19 pandemic was evaluated using five items adapted from Hsu et al. [9] and Knapp [32]. Mandatoriness was assessed using four items adapted from Boss et al. [13], while extrarole behaviors were assessed using six items adapted from Hsu et al. [9]. Security policy specification was evaluated to measure how specifically the policies were defined using nine items adapted from Hsu et al. [9], Boss et al. [13], and D’Arcy et al. [8]. Reward was assessed to measure the degree of compensation allotted to the employees for complying with security policies using four items adapted from Hsu et al. [9] and Boss et al. [13]. The severity and certainty of the sanctions were evaluated using five and six items, respectively, adapted from D’Arcy and Devaraj [11]. Moral belief was assessed using five items adapted from D’Arcy and Devaraj [11] (Table 3).

2.3.3. Validity and Reliability. As shown in Table 4, a confirmatory factor analysis was conducted to test the unidimensionality of the measurements. A set of measured
### Table 2: Demographic information of respondents.

| Survey participants (N = 207) | n  | %    |
|-------------------------------|----|------|
| Gender                        |    |      |
| Male                          | 166| 80.2 |
| Female                        | 40 | 19.3 |
| Missing                       | 1  | 0.5  |
| Age                           |    |      |
| 26–30                         | 27 | 13.0 |
| 31–35                         | 32 | 15.5 |
| 36–40                         | 50 | 24.2 |
| 41 and over                   | 97 | 46.9 |
| Missing                       | 1  | 0.5  |
| Tenure (years)                |    |      |
| 1–3                           | 35 | 16.9 |
| 4–6                           | 22 | 10.5 |
| 7–10                          | 28 | 13.5 |
| 10 and over                   | 121| 58.5 |
| Missing                       | 1  | 0.5  |
| Position                      |    |      |
| Managerial                    | 3  | 1.4  |
| Technical                     | 147| 71.0 |
| Professional staff            | 25 | 12.1 |
| Administrative                | 31 | 15.0 |
| Missing                       | 1  | 0.5  |
| Department                    |    |      |
| Security                      | 66 | 31.9 |
| Others                        | 141| 66.2 |
| Missing                       | 4  | 1.9  |
| Industry type                 |    |      |
| Manufacturing                 | 1  | 0.5  |
| IT                            | 82 | 39.6 |
| Finance                       | 105| 50.7 |
| Others                        | 18 | 8.7  |
| Missing                       | 1  | 0.5  |
| Company size                  |    |      |
| Less than 100                 | 14 | 6.8  |
| 100–499                       | 64 | 30.9 |
| 500–999                       | 6  | 2.9  |
| 1000–3000                     | 67 | 32.4 |
| 5000–9999                     | 6  | 2.9  |
| More than 9999                | 35 | 16.9 |
| Missing                       | 2  | 1.0  |

### Table 3: Survey scale items adapted to telecommuting.

| Measurement variables | Item                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Items on effectiveness of telecommuting security policies adapted from Hsu et al. [9] and Knapp [32] | In general, information in the organization is sufficiently protected while telecommuting. Overall, the telecommuting information security policy is effective. The telecommuting information security policy achieves most of its goals. The telecommuting information security policy accomplishes its most important objectives. The telecommuting information security policy has kept security losses to a minimum. |
| Policy effectiveness 01 |                                                                                                                                                                                                     |
| Policy effectiveness 02 |                                                                                                                                                                                                     |
| Policy effectiveness 03 |                                                                                                                                                                                                     |
| Policy effectiveness 04 |                                                                                                                                                                                                     |
| Policy effectiveness 05 |                                                                                                                                                                                                     |
| Items on mandatoriness adapted from Boss et al. [13] | I am required to secure my system according to the organization’s documented policies and procedures while telecommuting. It is expected that I will take an active role in securing my computer from cyberattacks (e.g., hacking, virus infection, and data corruption) while telecommuting. There is an understanding that I will comply with the organizational security policies and procedures regarding telecommuting. Regulatory compliance requirements (e.g., FERPA, HIPAA, and Sarbanes-Oxley) motivate me to follow the organization’s IT security policies, procedures, and guidelines regarding telecommuting to the best of my ability. |
| Mandatoriness 01 |                                                                                                                                                                                                     |
| Mandatoriness 02 |                                                                                                                                                                                                     |
| Mandatoriness 03 |                                                                                                                                                                                                     |
| Mandatoriness 04 |                                                                                                                                                                                                     |
Table 3: Continued.

| Measurement variables | Item |
|------------------------|------|
| Items on specification adapted from Hsu et al. [9], Boss et al. [13], and D’Arcy et al. [8] | |
| Specification 01 | There are written rules on the security policies and procedures followed by the organization regarding telecommuting. |
| Specification 02 | I am familiar with the organization’s IT security policies, procedures, and guidelines for telecommuting. |
| Specification 03 | The organization’s existing policies and guidelines cover how to protect my computer system while telecommuting. |
| Specification 04 | I am required to know many written procedures and general practices to secure my computer system while telecommuting. |
| Specification 05 | My organization has specific guidelines regarding the acceptable use of e-mail while telecommuting. |
| Specification 06 | My organization has established rules regarding the use of computer resources while telecommuting. |
| Specification 07 | My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use while telecommuting. |
| Specification 08 | My organization has specific guidelines regarding the acceptable use of computer passwords while telecommuting. |
| Specification 09 | My organization has specific guidelines that outline what employees can do with their computers while telecommuting. |
| Items on monitoring adapted from D’Arcy et al. [8] | |
| Monitoring 01 | I believe that my organization monitors any modification or alteration of computerized data while telecommuting. |
| Monitoring 02 | I believe that the computing activities of telecommuting employees are monitored by my organization. |
| Monitoring 03 | I believe that my organization monitors computing activities to ensure that employees perform only explicitly authorized tasks while telecommuting. |
| Monitoring 04 | I believe that my organization regularly reviews the system logs of telecommuting employees. |
| Monitoring 05 | I believe that my organization conducts periodic audits to detect the use of unauthorized software on its computers. |
| Monitoring 06 | I believe that my organization actively monitors the content of e-mail messages exchanged by telecommuting employees. |
| Items on reward adapted from Hsu et al. [9] and Boss et al. [13] | |
| Reward 01 | I will receive a personal mention in oral or written reports if I comply with the security policies and procedures at this organization while telecommuting. |
| Reward 02 | I will be given monetary or nonmonetary rewards for following security policies and procedures while telecommuting. |
| Reward 03 | Tangible rewards depend on whether I follow the organization’s IT security policies, procedures, and guidelines while telecommuting. |
| Reward 04 | My pay raise and/or promotion depend on whether I follow the documented security policies and procedures while telecommuting. |
| Items on extrarole behavior adapted from Hsu et al. [9] | |
| Extrarole 01 | Employees of this department volunteer to engage in security policy-related behaviors while telecommuting. |
| Extrarole 02 | Employees of this department help each other to learn about the telecommuting security policies. |
| Extrarole 03 | Employees of this department help orient new employees to the telecommuting security policies. |
| Extrarole 04 | Employees of this department develop and make recommendations concerning telecommuting information security policies that affect the entire organization. |
| Extrarole 05 | Employees of this department speak up and encourage others in the organization to become more involved in telecommuting information security policies that affect the entire organization. |
| Extrarole 06 | Employees of this department voice their opinion about new strategies or changes made to the telecommuting information security policies. |
| Items on perceived severity adapted from D’Arcy and Devaraj [11] | |
| Perceived severity 01 | Severe responsibilities should be taken for accessing personnel systems using administrator passwords while telecommuting. |
| Perceived severity 02 | Accessing unauthorized systems while telecommuting will result in disciplinary action. |
| Perceived severity 03 | Severe responsibilities should be taken for revising personal overtime records using administrator passwords while telecommuting. |
| Perceived severity 04 | Severe responsibilities should be taken for installing unauthorized software on corporate computers while telecommuting. |
| Perceived severity 05 | Severe responsibilities should be taken for sending inappropriate emails to colleagues from the corporate email account while telecommuting. |
| Items on perceived certainty adapted from D’Arcy and Devaraj [11] | |
| Perceived certainty 01 | Accessing personnel systems using administrator passwords while telecommuting will be discovered. |
| Perceived certainty 02 | It is likely that companies will detect the employees who access unauthorized systems while telecommuting. |
| Perceived certainty 03 | Revising personal overtime records using administrator passwords while telecommuting will be discovered. |
| Perceived certainty 04 | Installing unauthorized software on corporate computers while telecommuting will be discovered. |
values, such as CMIN (Minimum Chi-square), DF (Degree of Freedom), $p$, RMR (Root-Mean-Square Residual), GFI (Goodness-of-Fit Index), AGFI (Adjusted Goodness-of-Fit Index), CFI (Comparative Fit Index), NFI (Normed Fit Index), and RMSEA (Root Mean Square Error of Approximation), was used to assess the fit of the model to the data. To get the optimal value of reliability, problematic items with squared multiple correlation (SMC) values less than 0.4 in the initial question were dropped, and the process was repeated until the desired result was achieved.

Our measurement model was analyzed based on the aforementioned confirmatory factor analysis, and the results are presented in Table 5. After optimizing the adequacy of the survey questions based on the SMC values, our data yielded the following results: CMIN = 141.727, DF = 99, $p \leq 0.001$, GFI = 0.934, AGFI = 0.886, CFI = 0.987, RMR = 0.046, NFI = 0.959, IFI = 0.987, and RMSEA = 0.046. The value of $p$ was found to be negative. However, the fit can be considered to be acceptable because the values of GFI, AGFI, CFI, NFI, and IFI were greater than 0.9 (note that AGFI was larger than 0.85), the value of RMR was less than 0.05, and the value of RMSEA was less than 0.1. As seen from Table 5, Cronbach’s alpha was greater than 0.7 (i.e., between 0.883 and 0.949), which indicates that the items have high internal consistency.

As shown in Table 6, a reliability analysis was performed using two tests: convergent validity and discriminant validity. Construct reliability was used to assess the convergent validity [33], and the average variance extracted (AVE) was used to assess the discriminant validity [34]. The construct reliability values obtained were greater than 0.7, which establishes convergent validity. Moreover, the AVE of all constructs was found to be greater than the square root of the largest correlation coefficient (which is 0.621 in this case), which establishes discriminant validity according to the criterion of Fornell and Larcker [34].

3. Results

This model was created with the assumption that the parameters shown to have the most influence in the existing research models in literature review would indicate different influences in telecommuting. Initially, we considered SETA

### Table 3: Continued.

| Measurement variables | Item |
|-----------------------|------|
| Perceived certainty 05 | It is likely that companies will detect the employees who install unauthorized software on corporate computers while telecommuting. |
| Perceived certainty 06 | Sending inappropriate emails to colleagues from the corporate email account while telecommuting will be discovered. |
| Items on moral belief adapted from D’Arcy and Devaraj [11] | |
| Moral belief 01 | If the password to a system that contains the payroll information of all employees is known, then it is morally permissible to access the system while telecommuting. |
| Moral belief 02 | It is morally permissible to revise personal overtime records using administrator passwords while telecommuting. |
| Moral belief 03 | It is morally permissible to install unauthorized software on corporate computers while telecommuting. |
| Moral belief 04 | It is morally permissible to send inappropriate emails to colleagues from the corporate email account while telecommuting. |

### Table 4: Measurement validity and reliability.

| Constructs | Attempts | Numbers | CMIN | DF | $p$ | RMR | GFI | AGFI | CFI | NFI | RMSEA |
|------------|----------|---------|------|----|-----|-----|-----|------|-----|-----|-------|
| Effectiveness | First | 5 | 27.667 | 5 | $p \leq 0.001$ | 0.023 | 0.953 | 0.858 | 0.982 | 0.978 | 0.148 |
| | Final | 4 | 4.050 | 2 | 0.132 | 0.008 | 0.990 | 0.952 | 0.998 | 0.996 | 0.071 |
| Mandatoriness | First | 4 | 5.769 | 2 | 0.056 | 0.021 | 0.986 | 0.932 | 0.993 | 0.989 | 0.096 |
| | Final | 4 | 5.769 | 2 | 0.056 | 0.021 | 0.986 | 0.932 | 0.993 | 0.989 | 0.096 |
| Specification | First | 9 | 155.655 | 27 | $p \leq 0.001$ | 0.868 | 0.856 | 0.761 | 0.923 | 0.909 | 0.152 |
| | Final | 5 | 10.912 | 5 | 0.053 | 0.023 | 0.980 | 0.941 | 0.993 | 0.988 | 0.076 |
| Monitoring | First | 6 | 39.007 | 9 | $p \leq 0.001$ | 0.073 | 0.938 | 0.855 | 0.972 | 0.965 | 0.127 |
| | Final | 5 | 10.848 | 5 | 0.054 | 0.042 | 0.981 | 0.942 | 0.993 | 0.987 | 0.075 |
| Reward | First | 4 | 22.979 | 2 | $p \leq 0.001$ | 0.093 | 0.944 | 0.722 | 0.974 | 0.972 | 0.226 |
| | Final | 4 | 22.979 | 2 | $p \leq 0.001$ | 0.093 | 0.944 | 0.722 | 0.974 | 0.972 | 0.226 |
| Perceived severity | First | 5 | 59.916 | 5 | $p \leq 0.001$ | 0.118 | 0.901 | 0.704 | 0.937 | 0.932 | 0.231 |
| | Final | 4 | 2.376 | 2 | 0.305 | 0.024 | 0.994 | 0.971 | 0.999 | 0.996 | 0.030 |
| Perceived certainty | First | 6 | 135.860 | 9 | $p \leq 0.001$ | 0.091 | 0.812 | 0.561 | 0.887 | 0.880 | 0.262 |
| | Final | 4 | 5.655 | 2 | 0.059 | 0.030 | 0.987 | 0.936 | 0.994 | 0.991 | 0.094 |
| Moral belief | First | 4 | 46.914 | 2 | $p \leq 0.001$ | 0.043 | 0.919 | 0.596 | 0.958 | 0.957 | 0.330 |
| | Final | 4 | 46.914 | 2 | $p \leq 0.001$ | 0.043 | 0.919 | 0.596 | 0.958 | 0.957 | 0.330 |
| Extrarole | First | 6 | 101.514 | 9 | $p \leq 0.001$ | 0.120 | 0.846 | 0.640 | 0.927 | 0.921 | 0.223 |
| | Final | 4 | 0.102 | 2 | 0.950 | 0.003 | 1.000 | 0.999 | 1.000 | 1.000 | 0.000 |
The proposed hypotheses were tested using structural equation modeling, which was performed using Analysis of Moment Structures (AMOS), a widely used statistical software package, along with LISREL: LISREL is a representative program for a long time, but it is difficult to use than AMOS. AMOS was selected for its convenient graphical user interface (GUI) compared to LISREL, in which users are required to create separate data files for each model. Also, AMOS is free for data compatibility with SPSS and Excel. As shown in Table 7, our proposed model shows how the impact of control factors under normal circumstances differs in a different working environment, namely, telecommuting. As seen from Figure 2 and Table 8, the estimates from the structural equation modeling are within tolerable levels for the proposed model, such that $CMIN = 142.987$, $CMIN/DF = 1.388$, $p = 0.006$, $GFI = 0.933$, $AGFI = 0.889$, $CFI = 0.988$, $RMR = 0.051$, $RMSEA = 0.043$, $NFI = 0.959$, and $IFI = 0.988$. The values of chi-square were found to be negative. However, the model-fit can be considered to be acceptable with comparison to Table 9 because the values of GFI, AGFI, CFI, NFI, and IFI were greater than 0.9 (note that AGFI was larger than 0.85) and the values of RMR and RMSEA were less than 0.1.

Our test results show that the proposed hypotheses H1a (0.590, critical ratio (C.R.) = 8.150), H1b (0.508, C.R. = 3.885), H3b (0.429, C.R. = 7.397), and H7 (1.180, C.R. = 9.021) are supported within a 95% confidence interval, with $p < 0.05$ and $C.R. > 1.96$.

However, the proposed hypotheses H2a (0.020, C.R. = 0.615), H2b (0.127, C.R. = 1.539), H3a (−0.012, C.R. =

---

**Table 5: Analysis of the measurement model.**

| Constructs   | M.V. a | R.W. b | S.R.W. c | S.E. d | C.R. e | M.E. f | SMC g | C.A. h |
|--------------|--------|--------|----------|--------|--------|--------|-------|-------|
| Effectiveness| 1.000  | 0.886  | 0.299    | 0.785  | 0.904  |
|             | 1.004  | 0.932  | 0.054    | 18.693 | 0.165  | 0.869  |
| Mandatoriness| 1.000  | 0.679  | 0.685    | 0.461  | 0.809  |
|             | 1.182  | 0.828  | 0.096    | 12.319 | 0.376  | 0.685  |
| Specification| 1.000  | 0.918  | 0.253    | 0.842  | 0.883  |
|             | 1.029  | 0.868  | 0.057    | 18.165 | 0.466  | 0.754  |
| Monitoring   | 1.000  | 0.882  | 0.594    | 0.777  | 0.912  |
|             | 1.126  | 0.951  | 0.074    | 15.280 | 0.275  | 0.905  |
| Reward       | 1.000  | 0.954  | 0.355    | 0.910  | 0.930  |
|             | 0.938  | 0.910  | 0.052    | 18.136 | 0.659  | 0.828  |
| Perceived severity | 1.000  | 0.957  | 0.148    | 0.917  | 0.935  |
|             | 0.935  | 0.917  | 0.047    | 19.754 | 269    | 0.841  |
| Perceived certainty | 1.000  | 0.887  | 0.336    | 0.787  | 0.907  |
|             | 1.088  | 0.936  | 0.061    | 17.719 | 0.210  | 0.875  |
| Moral belief  | 1.000  | 0.983  | 0.099    | 0.966  | 0.949  |
|             | 0.872  | 0.922  | 0.068    | 12.751 | 0.374  | 0.849  |
| Extrarole    | 1.000  | 0.933  | 0.397    | 0.871  | 0.943  |
|             | 0.995  | 0.956  | 0.046    | 21.729 | 0.250  | 0.914  |

**Table 6: Validation of the measurement model.**

| Constructs  | 1       | 2       | 3       | 4       | 5       | 6       | 7       | 8       | 9       |
|-------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| (1) Effectiveness | 1.00   |        |        |        |        |        |        |        |        |
| (2) Mandatoriness  | 0.708  | 1.00   |        |        |        |        |        |        |        |
| (3) Specification   | 0.788  | 0.716  | 1.00   |        |        |        |        |        |        |
| (4) Monitoring      | 0.494  | 0.472  | 0.516  | 1.00   |        |        |        |        |        |
| (5) Perceived severity | 0.445  | 0.553  | 0.536  | 0.480  | 1.00   |        |        |        |        |
| (6) Moral belief    | −0.055 | −0.1   | −0.012 | −0.008 | −0.122 | 1.00   |        |        |        |
| (7) Perceived certainty | 0.545  | 0.596  | 0.646  | 0.459  | 0.663  | −0.103 | 1.00   |        |        |
| (8) Reward          | 0.275  | 0.201  | 0.302  | 0.343  | 0.269  | 0.322  | 0.210  | 1.00   |        |
| (9) Extrarole       | 0.469  | 0.409  | 0.537  | 0.487  | 0.416  | 0.084  | 0.380  | 0.592  | 1.00   |
| Construct reliability | 0.923  | 0.955  | 0.814  | 0.798  | 0.894  | 0.885  | 0.859  | 0.775  | 0.847  |
| AVE a              | 0.781  | 0.643  | 0.936  | 0.663  | 0.808  | 0.793  | 0.752  | 0.634  | 0.734  |

aAverage variance extracted.
We observe that specification indirectly affects telecommuting security policies via mandatoriness, which corresponds to a \( p \) value of 0.007. As seen from Table 10, we also investigated the moderating effect of the department (i.e., information security and other departments) on our hypotheses. Note that the difference in the number of degrees of freedom (DF) between the constrained and unconstrained models was 14 and the reduced chi-squared value (36.492) was greater than the corresponding reference value (23.68). Moderating effects were found to be significant (with \( p = 0.001 \)). In particular, specification had a stronger effect on mandatoriness in the information security department compared to other departments.

Regarding the effect of sanctions on extrarole behaviors, the certainty of sanctions was more important in the information security department, whereas the severity of sanctions was more effective in other departments. In addition, specification affected more positively extrarole behaviors in the information security department than in other departments. Furthermore, reward affected intensely extrarole behaviors in the information security department than in other departments. Finally, mandatoriness was more effective in departments other than the information security department.

Specification of telecommuting security policies was found to directly affect mandatoriness and extrarole behaviors (H1a and H1b). Mandatoriness improved the effectiveness of telecommuting security policies (H7), and reward was found to directly influence extrarole behaviors (H3b). However, extrarole behaviors did not improve the effectiveness of telecommuting security policies (H8). Finally, specification had an indirect influence on the effectiveness of telecommuting security policies.

4. Discussion
In this study, we examined how the security control factors in a well-organized office environment are affected in a
| Path (hypothesis)          | Estimate | C.R. \(^a\) | \(p\) \(^b\) | Estimate | \(p\) \(^b\) |
|---------------------------|----------|-------------|-------------|----------|-------------|
| Specification \(\rightarrow\) mandatoriness | 0.590    | 8.150       | ***         |          |             |
| Specification \(\rightarrow\) extrarole   | 0.508    | 3.885       | ***         |          |             |
| Monitoring \(\rightarrow\) mandatoriness  | 0.020    | 0.615       | 0.539       |          |             |
| Monitoring \(\rightarrow\) extrarole   | 0.127    | 1.539       | 0.124       |          |             |
| Reward \(\rightarrow\) mandatoriness    | -0.012   | -0.514      | 0.608       |          |             |
| Reward \(\rightarrow\) extrarole   | 0.429    | 7.397       | ***         |          |             |
| Perceived severity \(\rightarrow\) mandatoriness | 0.015    | 0.357       | 0.721       |          |             |
| Perceived severity \(\rightarrow\) extrarole | 0.119    | 1.119       | 0.263       |          |             |
| Perceived certainty \(\rightarrow\) mandatoriness | 0.033    | 0.549       | 0.583       |          |             |
| Perceived certainty \(\rightarrow\) extrarole | -0.138   | -0.943      | 0.346       |          |             |
| Moral belief \(\rightarrow\) mandatoriness | -0.026   | -1.163      | 0.245       |          |             |
| Moral belief \(\rightarrow\) extrarole | -0.083   | -1.492      | 0.136       |          |             |
| Mandatoriness \(\rightarrow\) effectiveness | 1.180    | 9.201       | ***         |          |             |
| Extrarole \(\rightarrow\) effectiveness | 0.034    | 0.882       | 0.378       |          |             |
| Specification \(\rightarrow\) effectiveness |          | 0.794       | 0.007       |          |             |
| Monitoring \(\rightarrow\) effectiveness |          | 0.039       | 0.426       |          |             |
| Reward \(\rightarrow\) effectiveness |          | 0.001       | 0.952       |          |             |
| Perceived severity \(\rightarrow\) effectiveness |          | 0.026       | 0.592       |          |             |
| Perceived certainty \(\rightarrow\) effectiveness |          | 0.036       | 0.644       |          |             |
| Moral belief \(\rightarrow\) effectiveness |          | -0.053      | 0.124       |          |             |

Model-fit\(^c\)  
CMIN = 142.987, CMIN/DF = 1.388, \(p\) = 0.006, GFI = 0.933, AGFI = 0.889, CFI = 0.988, RMR = 0.051, RMSEA = 0.043, NFI = 0.959, IFI = 0.988

\(^a\)C.R. > 1.96; \(^b\)\(p\) < 0.05; \(^c\)Model-Fit Reference Value: CMIN/DF (<2), \(p\) > 0.05, GFI (≥0.9), AGFI (≥0.85), CFI (≥0.9), NFI (≥0.9), RMR (≤0.1), and RMSEA (≤0.1).
telecommuting environment, which has become extremely common during the COVID-19 pandemic. Our analysis revealed that mandatoriness is a significant determinant of the effectiveness of telecommuting security policies compared to extrarole behaviors, which were considered to be more important by Hsu et al. [9]. It appears that working in an isolated space, separated from other employees, has a relatively variable effect. Our results confirmed that given the importance of mandatoriness in telecommuting environments, compulsory measures involving security technologies (e.g., virtual private network, one-time password, and virtual desktop infrastructure) should be implemented urgently. Moreover, it is recommended that organizations give more importance to their security control policies, such as prohibiting the use of screen capture tools and the data being stored into personal computers while teleworking.

4.1. Research Contributions. Our study mainly focused on the effects of various control factors on corporate security policies in uncharted working environment caused by the COVID-19 pandemic. The employees of an organization serve an important role by driving one another to keep the office environment well organized and under control. However, they do not play a crucial role in telecommuting environments because they cannot serve the same purpose being isolated from social pressure. Therefore, mandatoriness was found to affect intensely telecommuting security policies than extrarole behaviors. Furthermore, specification was found to play a crucial role in affecting mandatoriness compared to other control factors.

In addition, our findings show that telecommuting tends to cause moral hazard as well as awareness among employees to avoid sanctions and monitoring by organizations. Interestingly, we found that reward has a critical impact on extrarole behaviors, which agrees with the Korean culture of “saving face.”

Our study also found that different departments, including information security department and other departments, had different moderating effects. As shown in Table 10, factors such as specification, sanctions, reward, and mandatoriness differed depending on the department duties. Our study contributes to the current research on security policy-making processes and shows that security policymakers need to consider developing new policies beyond conventional security programs.

4.2. Limitations and Future Research. Our study has a few limitations, which we discuss here. First, the use of a subjective assessment from respondents who telecommuted during the COVID-19 pandemic could lead to common method bias. This is because there is always a possibility that some respondents could have replied differently regarding the security controls in teleworking being better than those in conventional office environments. Thus, it would be better for future studies to examine the effects of control factors based on a variety of datasets that result from actual security policy violations.

Second, we conducted the present study by measuring how each control item applies specifically to the teleworking environment. Therefore, it remains unclear whether our measurement items would be applicable to a completely different environment.

Finally, the research data for this work were collected from organizations in Korea, especially from financial companies, where security controls are well organized compared to other companies. However, telecommuting was not popular in Korea before the COVID-19 pandemic owing to the restrictions of network segmentation. Thus,
employees were not familiar with the concept of teleworking. Moreover, security controls were newly applied to teleworking because of the pandemic, and most employees have still not adapted themselves to the new work environment. Consequently, particular care must be taken before generalizing our findings to new office or telecommuting environments.

After the experience of telecommuting, we need to revalidate our model 1 or 2 years thereafter, and we also encourage research in environment where workers have already been telecommuting for a long time to compare our models.

5. Conclusions

In this study, we examined the factors affecting corporate security policies in the new telecommuting environment created by the COVID-19 pandemic. Cybersecurity threats are increasing exponentially with the sudden increase in teleworking. Despite existing security controls, more compelling cybersecurity risks keep threatening telecommuters. Thus, we need to continue searching for the critical determinants of security control factors in telecommuting environments. The data collected from 207 telecommuting employees through Google surveys in this work indicate that specification and mandatoriness play a decisive role in making telecommuting security policies more effective. Therefore, we suggest that corporations should take administrative and technical measures to guard against unexpected dangers and reinforce their security policies associated with the teleworking environment.

Data Availability

The Excel data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors would like to thank Editage (https://www.editage.co.kr) for English language editing. This study was supported by a grant of the Korean Heath Technology R&D Project, Ministry of Health and Welfare, Republic of Korea (HI19C0866).

References

[1] U.S. Bureau of Labor Statistics, TED: The Economics Daily, https://www.bls.gov/opub/ted/2019/29-percent-of-wage-and-salary-workers-could-work-at-home-in-their-primary-job-in-2017-18.htm Research Report, 2019.
[2] J. Lavelle, Gartner CFO Survey Reveals 74 remote Work Permanently, https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-survey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work- perennially Research Report, 2020.
[3] M. Baker, Gartner Survey Reveals 82 to Work Remotely Some of the Time, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time Research Report, 2020.
[4] Korea Internet and Security Agency, Kisa Cyber Threat Report Q2 2020, http://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35506 Research Report, Korea Internet and Security Agency, Seoul, South Korea, 2020, http://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35506 Research Report.
[5] C. Johnson, B. Khadka, R. B. Basnet, and T. Doleck, “Towards detecting and classifying malicious urls using deep learning,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 11, no. 4, pp. 31–48, 2020.
[6] A. Abhishta, W. V. Heeswijk, M. Junger, J. M. Lambert, I. Nieuwenhuis, and R. Joosten, "Why would we get attacked? an analysis of attacker's aims behind DDoS attacks," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 11, no. 2, pp. 3–22, 2020.
[7] C. Rubinstein, Beware: Remote Work Involves These 3 Cyber Security Risks, http://www.forbes.com/sites/carrierubinstein/2020/04/10/beware-remote-work-involves-these-3-cyber-security-risks/?sh=17e6b176fe4 Research Report, 2020.
[8] J. D’Arcy, A. Hayow, and D. Galletta, “User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach,” Information Systems Research, vol. 20, no. 1, pp. 79–98, 2009.
[9] J. S.-C. Hsu, S.-P. Shih, Y. W. Hung, and P. B. Lowry, “The role of extra-role behaviors and social controls in information security policy effectiveness,” Information Systems Research, vol. 26, no. 2, pp. 282–300, 2015.
[10] S. M. Lee, S.-G. Lee, and S. Yoo, “An integrative model of computer abuse based on social control and general deterrence theories,” Information and Management, vol. 41, no. 6, pp. 707–718, 2004.
[11] J. D’Arcy and S. Devaraj, “Employee misuse of information technology resources: testing a contemporary deterrence model,” Decision Sciences, vol. 43, no. 6, pp. 1091–1124, 2012.
[12] D. John Lemay, R. B. Basnet, and T. Doleck, “Examining the relationship between threat and coping appraisal in phishing detection among college students,” Journal of Internet Services and Information Security, vol. 10, no. 1, pp. 38–49, 2020.
[13] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, “If someone is watching, I’ll do what I’m asked: mandatoriness, control, and information security,” European Journal of Information Systems, vol. 18, no. 2, pp. 151–164, 2009.
[14] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness,” MIS Quarterly, vol. 34, no. 3, pp. 523–548, 2010.
[15] C. Posey, T. L. Roberts, P. B. Lowry, R. J. Bennett, and J. F. Courtney, “Insiders’ protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors,” MIS Quarterly, vol. 37, no. 4, pp. 1189–1210, 2013.
[16] J. D. Wall, P. Palvia, and P. B. Lowry, “Control-related motivations and information security policy compliance: the role of autonomy and efficacy,” Journal of Information Privacy and Security, vol. 9, no. 4, pp. 52–79, 2013.
[17] M. E. Whitman, A. M. Townsend, and R. J. Aalberes, “Information systems security and the need for policy,”
[18] T. L. Wiant, *Policy and its Impact on Medical Record Security*, University of Kentucky, Lexington, KY, USA, 2003.

[19] T. K Das and B.-S. Teng, “Between trust and control: developing confidence in partner cooperation in alliances,” *Academy of Management Review*, vol. 23, no. 3, pp. 491–512, 1998.

[20] K. M. Eisenhardt, “Control: organizational and economic approaches,” *Management Science*, vol. 31, no. 2, pp. 134–149, 1985.

[21] L. J. Kirsch, “Deploying common systems globally: the dynamics of control,” *Information Systems Research*, vol. 15, no. 4, pp. 374–395, 2004.

[22] V. K. G. Lim, T. S. H. Teo, and G. L. Loo, “How do i loaf here? let me count the ways,” *Communications of the ACM*, vol. 45, no. 1, pp. 66–70, 2002.

[23] J. Luft, “Bonus and penalty incentives contract choice by employees,” *Journal of Accounting and Economics*, vol. 18, no. 2, pp. 181–206, 1994.

[24] N. Dopuch, J. G. Birnberg, and J. S. Demski, *Cost Accounting: Accounting Data for Management's Decisions*, Harcourt Brace Jovanovich, San Diego, CA, USA, 1974.

[25] D. W. Straub and R. J. Welke, “Coping with systems risk: security planning models for management decision making,” *MIS Quarterly*, vol. 22, no. 4, pp. 441–469, 1998.

[26] R. F. James and W. Waller, “Carrot or stick? contract frame and use of decision-influencing information in a principal-agent setting,” *Journal of Accounting Research*, vol. 43, no. 5, pp. 709–733, 2005.

[27] P. Raymond, “How much do we really know about criminal deterrence,” *Journal of Criminal Law and Criminology*, vol. 100, pp. 765–824, 2010.

[28] T. C. Pratt, F. T. Cullen, R. B. Kristie, L. E. Daigle, and D. M. Tamara, "The Empirical status of deterrence theory: a meta-analysis," *Taking Stock: The Status of Criminological Theory*, American Psychological Association, Washington, DC, USA, 2006.

[29] L. A. Ellis and S. S. Simpson, “Informal sanction threats and corporate crime: additive versus multiplicative models,” *Journal of Research in Crime and Delinquency*, vol. 32, no. 4, pp. 399–424, 1995.

[30] B. Chae and M. S. Poole, “Mandates and technology acceptance: a tale of two enterprise technologies,” *The Journal of Strategic Information Systems*, vol. 14, no. 2, pp. 147–166, 2005.

[31] M. D. Jill, “Financial accountants' perceptions of management's ethical standards,” *Journal of Business Ethics*, vol. 31, no. 3, pp. 233–244, 2001.

[32] K. J. Knapp, "A model of managerial effectiveness in information security: from grounded theory to empirical test," Technical Report, Auburn University, Auburn, AL, USA, 2005.

[33] J. F. Hair, R. E. Anderson, R. L. Tatham, and W. C. Black, *Multivariate Data Analysis*, Englewood Cliff, NJ, USA, 2019.

[34] C. Fornell and D. F. Larcker, “Evaluating structural equation models with unobservable variables and measurement error,” *Journal of Marketing Research*, vol. 18, no. 1, pp. 39–50, 1981.