International Journal of Advanced Culture Technology Vol.10 No.2 307-313 (2022)
DOI https://doi.org/10.17703/IJACT.2022.10.2.307

IJACT 22-6-40

Research on Security Threats for SMEs by Workplace in the COVID-19 Environment

[1]Woo-Su Kim, [2]Heon-Wook Lim

[1]Director., Division of Social Value Promotion, KEIT, Korea
[2]Prof., Division of Padeia, Sungkyul Univ., Korea
kws@keit.re.kr, 3795879@hanmail.net

Abstract

Although telecommuting of SMEs has been activated due to the COVID-19 phenomenon, the security model for this is insufficient. Accordingly, the study was divided into threats centered on smartphones and threats centered on smartphone users. As a result of the study, one-third of SMEs are working from home. At this company with 100 employees, more than 50% of them work from home.and In the metal, machinery and chemical industries with factories, 20% of them work from home. As a result of analyzing the correlation between telecommuting according to the presence or absence of a factory, the correlation coefficient (r=-.385) has a clear linear relationship. And, as a result of the regression analysis, the R-squared value was 0.148, so companies with factories are highly related to telecommuting. In other words, we found that SMEs with factories do not want to work from home. In addition, as a result of analyzing the level of security threats, there were great concerns about theft, hacking, and phone taking during remote work. As limitations of the study, there were difficulties in selecting SMEs from the population in a non-face-to-face work environment, and there were limitations in the questionnaire items for deriving a non-face-to-face work environment.

Keywords: *COVID 19, Non-face-to-face work environment, Work from home, Security model, Correlation analysis*

1. INTRODUCTION

1.1 Purpose of Research

COVID-19 has made businesses more active at home and Work is turning into a smart work environment. However, the security model cannot keep up with the working environment at home. Smart-work does not determine a specific place of work. And it is to perform business using an information and communication network. Therefore, it can be defined as including working from home, working in a smart work center, and working on a mobile[1]. According to a 2020 SMEs technical protection survey, 75.3% of companies do not have non-face-to-face business regulations. and 81.4% of companies neglect to manage from home workers. Therefore, we want to create measures against the technology leakage of SMEs in non-face-to-face work, and find security threats by remote access type.

Manuscript received: May 28, 2022 / revised: June 5, 2022 / accepted: June 9, 2022
Corresponding Author: 3795879@hanmail.net
Tel: +82-031-450-5161
Professor, Dept. of Liberal Arts, Hansei Univ., Korea

1.2 Research Progress Order

The Order of Study Progress is to create questionnaires that differentiate from existing research, such as (Table 1), and to increase the validity and reliability of the data. In addition, The research was also conducted for the purpose to offer security measures for each company.

Table 1. Research Progress Procedure

Review data	Surveys	Results Analysis
◦ Purpose and need for data review - Purpose of deriving questions to use in surveys - Needed to differentiate itself from existing research ◦ Data review direction - Security Vulnerability Research - Research on security vulnerability measures - Investigating threats from this study	◦ Reasons for conducting surveys - Feasibility and evidence of research - Various voices in the field ◦ Survey methods and directions - Development of questionnaires through Delphi Method - Determine the level of security activities of threats due to corporate status (industry, business)	◦ Results analysis direction - Identify corporate characteristics - Identify threats in non-face-to-face work - Proposed measures by company characteristics

2. PRIOR RESEARCH

There were three types of prior studies to look for security threats caused by the remote work of SMEs. First, it is a case of studying vulnerabilities and countermeasures in a security environment. That is, DRM log analysis, ICS(industrial control system), SDN controller, and network separation were selected and security measures were also studied. Second, it is a case of researching each security threat by dividing the smart-phone hardware and software. Third, there were studies covering loss and risk exposure at the phone user center. Third, it is a case of studying loss and security threats that occur when a user's phone is used. This report will study security threats by home, movement, and smart-work center, depending on the location of the phone.

2.1 Security Vulnerability Research

In relation to security vulnerability research in non-face-to-face environments, Liu Hyun (2021) identified convergence security threats in five categories: cyber security, fake news, remote voting, remote work, and video security threats[2]. Limited number (2014) is a mobile cloud security threat that can be used to steal data, data loss, and account takeover. There are nine categories: service takeover, unsafe APIs, denial of service, malicious internal use, abuse of cloud services, lack of understanding of cloud services, and vulnerability to shared technologies[3].

2.2 Security Measures Research and Countermeasures

Studies that presented security vulnerability studies and countermeasures in non-face-to-face environments were divided by study. It was difficult to present detailed technology as a countermeasure and select it as a threat to general SMEs. In summary, industrial control systems (ICS), DRM log analysis, SDN controllers, Internet of Things communication technology, memory security, and net differentiation were the main

targets[4]. Lee Ji-seop (2020) is an industrial control system (ICS) that measures a variety of distributed assets, It consists of a monitoring and controlling system, and the required security measures suggested 10 things, including security audit (FAU), communications (FCO), password support (FCS), user data protection (FDP), identification and authentication (FIA), security management (FMT), TSF protection (FPT), resource utilization (FRU), resource access (FTA), and secure path /channel (FTP). Brown rice (2016) was intended to establish a process for predicting and proactively monitoring employees' retirement signs using DRM logs, and presented DRM utilization for control of attendance records, firewall logs, web access, and file transfer records[5]. Won Jong Hyuk (2018) wanted to study intrusion detection response technology using SDN Controller function to respond to security threats in IoT environments[6]. By adding an Open Flow-based SDN Controller to the network switch of the existing loT network, it was said that the effectiveness of the detection method through sampling techniques, and it was possible to monitor and attack the entire net week only by linking with IDS and IPS. Moon Hyung-jin (2016) wanted to analyze the Internet of Things communication technology Zig-Bee, Co AP, MQTT, and XMPP to derive security threats. Using a double authentication system that combines a physical device and a PIN as a countermeasure, the following methods were proposed. (enhanced location data transmission security of devices connected to IoT), (two people control passwords and operating systems together), (enhanced illegal device security), (using malware intrusion prevention and closed networks), (authentication), (network service), (encryption), (cloud security, (security configuration control), (software and firmware security)[7].

Lee Sang-won (2015) proposed a response to memory tampering because security threats such as (game data manipulation), (payment irregularities), (account use), and (leakage of personal information) are increasing at the same time. It proposed data encryption and data verification methods that applied the SHA512 algorithm to random numbers. Extract (SHA512 Digest), (which generates random numbers), (there is no decryption in the sum of random numbers), and difficult to guess the value seen in terms of algorithm ratio, (stored as an XOR key value), (extracted HASH) value is each an XOR key and the data to be secreted using this key value and XOR computation, decrypting the encrypted game money for verification up 2 seconds (XOR) compared to the two values are compared to each other to determine memory modulation when it is not matched is a method of applying a routine to end the game[8].

2.3 Smart-phone Security Threats and Countermeasures Research

The classification of security threats related to smart-phone security was divided into threats centered on smart-phones and threats centered on smart-phone users. For research on threats and countermeasures centered on smart-phones, Choi Young-jin (2014) wanted to divide into users, places, terminals, networks, servers and derive vulnerabilities by layer according to the service delivery system to identify the main risk area of mobile office service. Specifically, 1) Leakage by the user and countermeasures such as logon information, loss of IC card/token, influx of password malware, unauthorized connection to public network, exploitation by third parties, management hall, harmful S/W execution, change of terminal, 2) Internet disconnection, inability to access the Internet due to threats to place defects, equipment loss, equipment damage, information of unauthorized persons, 3) Unsuitable terminals, logical access control bypass, insecure security module, malware, log-on information exposure, encryption key loss, communication S/W misleathing, 4) Leakage from network: internet connection, insecure internet, data surveillance, data leakage, use of personalP2P arbitrary network, 5) Leaks from servers and threatened threats: it proposed server inaccessibility, excessive access rights, unauthorized server access, and vulnerability use information[9]. In connection with the study on security threats and countermeasures centered on smart-phone users, Jeon Ung-ryol (2011) was considered by dividing the inside of the smart-phone into applications, platforms, and smart-phone devices and dividing the outside of the smart-phone into networks, servers and base stations, and PCs[10].

2.4 Threats derived from this study

In this study, the security threat classification related to smart-phone security was divided into threats centered on smart-phones and threats centered on smart-phone users. It was divided into security threat elements by remote connection type according to the location of using the smart-phone as a separate method. There are six threats and a threat of ① documents being defamed (content changes). ② There is a threat of wiretapping. ③ There is damage to smart-phone shooting. ④ There is a threat of theft or loss. ⑤ There is a threat of hacking (printouts, USB, laptops, etc.). ⑥ There is a malware threat

3. DISCUSSION

3.1 Investigation

The population is targeted at 200 small and medium-sized enterprises with industrial technology.111 persons involved in the investigation (45 security officers, 27 computer managers, 39 technical protection experts). The development of the questionnaire was divided into three areas (when working from home, on the move, when working outside) according to the route of the development of the questionnaire by secondary modification through the Delphi Method for expert surveys. The method of statistics of questionnaires is to use spss statistical programs, frequency analysis, cross-analysis. In order to configure the questionnaire, the company's characteristics → the → of threats in non-face-to-face business, and the → measures proposed. Considerations include is There are disagreements between security officers and technical protection experts in the company regarding the threat of remote work. Cross-analysis to investigate differences of opinion by work and analyze the approach of type changes. Considering the type change of security work in non-face-to-face workplaces

3.2 Results

3.2.1 The Non-face-to-face Workplace and Security Threats of SMEs

Analysis Results as shown in (Table 2) of the analysis and correlation analysis to find out the characteristics of the company related to working from home, factory use and working from home have a strong correlation. The correlation factor (Pearson correlation, expressed in r) represents ±1, and if the correlation factor is zero, the correlation cannot be predicted. In general, the correlation factor is less than 0.1 (irrelevant), 0.1 ~ 0.3 (weak linear relationship), 0.3 ~ 0.7 (distinct quantitative linear relationship), 0.7 or more (strong linear relationship). The following results were obtained from table correlation analysis. The most correlated variable at the confidence interval 99% level (significance level of 1%) is telecommuting * factory ownership and the correlation factor (r) is -.385**. If there is a factory, it indicates that there is a distinct linear relationship with not working from home.

Table 2. Correlation Analysis : work from home, sales, number of employees, power, factory

Correlation coefficient		Working from home	Revenue	Factory presence or not
Working from home	Pearson factor	1	.045	-.385**
	Significance (both)		.707	.001
Revenue	Pearson factor		1	-.187
	Significance (both)			.115
Factory presence or not	Pearson factor			1
	Significance (both)			

**. The correlation factor is significant at the 0.01 level (both). Confidence interval 99% level (1% significance level)

3.2.2 Regression of Working from Home due to Factory Presence

Analysis results To find out the characteristics of companies related to working from home, a regression analysis can be found that factory stays affect the working of the home Regression analysis wants to determine how much dependent variables (factory duties, employees) affect dependent variables (with or without working from home) by identifying the influence between variables. In model medicine b, the R square shows the explanatory power of the regression analysis, and the closer the value is to 1, the higher the explanatory power. Next, Durbin-Wason has a value of 0 to 4 as a value indicating independence, and the closer to 2 is independence, and if it is 0 is a static relationship, 4 is in an adverb relationship. If the significance of the F check in the distributed analysis b is less than the significance level of 0.05, the regression model is adopted if the significance level in the appropriate coefficient is less than 0.05. (Table 3) regression results were obtained. As a result of the regression analysis of working from home according to the factory use, the R square value is highly explanatory at 0.148, Durbin-Wason value is independent to 2.061, and the significance of the F check is 0.001, and companies with factories with only a significance level of 0.05 may be said to be highly associated with working from home.

Table 3. regression results (work from home_factory or not)
: Independent variables are factory-available, dependent variables (work from home) House

Model Summary b	R	R Square	Modified R Squared	Standard error of estimates	Statistical volume change		Durbin -Watson
					R Square change	Significance Probability F Change	
1	.385a	.148	.136	.450	.148	.001	2.061

Distributed analysis b		Sum squared	freedom	Average squared	F	Significance Probability
1	Regression model Residual sum	2.460	1	2.460	12.171	.001a (suitable)
	Residual	14.151	70	.202		
	sum	16.611	71			

3.2.3 Degree of Security Threat

○ Requirements

The following questions are about security threats by remote work (remote access) form.
- Security threats on the go are theft threats (67.2%), malware (malware) threats (60.8%).
- Security threats when working outside the company are hacking (65.2%), von Psalm damage (63.4%), eavesdropping (61.8%), and malware (60.6).

○ Analysis results

- Frequency analysis of security threat factors by remote work (remote access) form
· On the move, this is in the following number: theft threat (67.2%), malware (malware) threat (60.8%).
· Outside work is investigated in order of hacking threat (65.2%) von Psychulhae threat (63.4%), eavesdropping threat (61.8%), and malware threat (60.6)

- Cross-analysis of security threat elements when working remotely
· Up species: Metals (64.8%) Pharmaceuticals (63.4%) Electronics (62.2%) Machinery (55.2%) Net

4. CONCLUSION

4.1 Main Analysis Results

4.1.1 Types of Technology Protection Business Changes in Non-face-to-face Environments

Unlike working from home to find out the type of work change, the proportion of remote work was surveyed at an average of 41.2% compared to the total work, and the information and communication industry with low factory retention was the highest at 1.37 times (51.20% average 33.00%).

- Analysis shows that working from home is carried out by one-third of SMEs, more than 1/2 of stable companies with more than 100 employees, and metal, machinery, and chemical industries with factories worked less than one-fifth less. In summary, working from home seems difficult to carry out for companies with factories and small businesses.

※ The correlation analysis result (r) related to working from home according to the factory operation has a distinct linear relationship with (-385), and the working from home * (employees -.169, up power.141) each had a low linear relationship. In other words, if you have a factory, you don't work from home.

※ As a result of the regression analysis of working from home according to the factory use, the R square value is highly explanatory at 0.148, Durbin-Wason value is 2.061 independence, and the significance of the F check is 0.001, and the company holding the factory with only a significance level of 0.05 can be said to be highly associated with working from home.

4.1.2 Security Threats in a Non-face-to-face Environment

To investigate the level of security threats felt by SMEs in non-face-to-face workplaces, After investigating the extent of threats to eavesdropping, phone shooting, loss, hacking, malware, etc., the security threat when working on the move is theft threat (67.2%), malware (malware) threat (60.8%), and security threat when working outside is hacking (65.2%), von 1 damage (63.4%), eavesdropping (61.8%), malware (60.6) net.

4.2 Limitations of Research

4.2.1 Difficulty Selecting SMEs in Non-face-to-face Workplaces

In the survey, the industry ① electronics, ② machine, ③ information communication, ④ metal, ⑤ chemicals, ⑥ Fiber, ⑦ Food products, ⑧ Bibi metal, ⑨ Pharmaceuticals, ⑩ Gita, etc., were divided into 10 types, but the industry was broad, and the industry related to non-face-to-face work was limited to information communications, so it was difficult to select recruiting groups. This is the limit of research.

4.2.2 Limits of Survey Items

In a survey to determine the status of damage in the non-face-to-face workplace, the government sought an

integrated approach by separating the office and the factory, but it lacked justification for representing the non-face-to-face workplace.

REFERENCES

[1] S. K. Park, G. Bong. Kim, G. J. Son, W. S. Lee, & J. P. Park, "A study on a security model for the establishment of a non-face-to-face smart work working environment in a physical network separation environment of public institutions", *Journal of the Korea Convergence Society*, Vol. 11. No. 10, pp. 37-44. 2020. https://doi.org/10.15207/JKCS.2020.11.10.037

[2] D. H. Yu, Y. U. Kim, Y. J. Ha, & Y. S. Ryu, "Consideration of New Convergence Security Threats and Countermeasures in the Zero-Contact Era", *Journal of the Korea Convergence Society*, Vol. 12, No. 1, pp. 1-9, 2021. https://doi.org/10.15207/JKCS.2021.12.1.001

[3] J. S. Han, "Security Threats in the Mobile Cloud Service Environment", *Journal of Digital Convergence*, Vol. 12, No. 5, pp. 263-269, 2014. http://dx.doi.org/10.14400/JDC.2014.12.5.263

[4] J. S. Lee, K. M. Park, & S. K. Kim, "A Study on Cyber Security Threat and Security Requirements for Industrial Wireless Communication Devices", *Journal of The Korea Institute of Information Security & Cryptology*, Vol. 30, No. 4, 2020.

[5] J. S. Lee, K. M. Park, & S. K. Kim, "A Study on Cyber Security Threat and Security Requirements for Industrial Wireless Communication Devices", *Journal of The Korea Institute of Information Security & Cryptology*, Vol. 30, No. 4, 2020.

[6] J. H. Won, J. W. Hong, & Y. Y. You, "A Study on the Improvement of Security Threat Analysis and Response Technology by IoT Layer", *Journal of Convergence for Information Technology*, Vol. 8, No. 6, pp.149-157, 2018.

[7] H. J. Mun, G. H. Choi, & Y. C. Hwang, "Countermeasure to Underlying Security Threats in IoT communication", *Journal of Convergence for Information Technology*, Vol. 2, pp. 37-44, 2026. http://dx.doi.org/10.22156/CS4SMB.2016.6.2.037

[8] S. W. Lee, H. K. Kim, & E. J. Kim, "A Study on Countermeasures for Personal Data Breach and Security Threats of Social Network Game", *Korea Game Society*, Vol. 15, No. 1, pp. 77-88, 2015.

[9] Y. J. Choi, J. H. Ra & D. I. Shin, "The Exploratory Study on Security Threats and Vulnerabilities for Mobile Office Environment", *Journal of Information Technology and Architecture*, Vol. 11. No. 2, pp. 175-185, 2014.

[10] W. R. Jeon, J. Y. Kim, Y. S. Lee, & D. H. Won, "Analysis of Threats and Countermeasures on Mobile Smartphone", *The Korean Society Of Computer And Information*, Vol. 16, No. 2, pp. 153-163, 2011.