International Journal of Advanced Culture Technology Vol.9 No.2 106-117 (2021)
DOI https://doi.org/10.17703/IJACT.2021.9.2.106

IJACT 21-6-14

A Study on Countermeasures Against Cyber Infringement Considering CPTED

[1] Heon-Wook Lim

[1]Prof., Dept. of Department of Liberal Arts, Hansei Univ., Korea
3795879@hanmail.net

Abstract

The aim is to find cyber measures in consideration of physical CPTED in order to prepare countermeasures for cybercrime prevention. For this, the six applied principles of CPTED were used as the standard. A new control item was created in connection with the control items of ISO27001. A survey was conducted on former and current investigators and security experts. As a result of the reliability analysis, the Kronbar alpha coefficient value was 0.947, indicating the reliability of the statistical value. As a result of factor analysis, it was reduced to six factors. The following are six factors and countermeasures. Nature monitoring blocks opportunities and strengthens business continuity. Access control is based on management system compliance, personnel security. Reinforcement of territoriality is reinforcement of each wife and ethics. Establishment of security policy to enhance readability, security system maintenance. Increasing usability is seeking ways to utilize, periodic incentives. For maintenance, security education is strength and security-related collective cooperation is conducted. The differentiation of this study was to find countermeasures against cybercrime in the psychological part of the past. However, they approached to find in cyber measures. The limitation of the study is to bring the concept of physical CPTED to the cyber concept.

Keywords: *CPTED, Cybercrime, Cyber-invasive, Reliability analysis, Factor analysis*

1. INTRODUCTION

1.1 Purpose of Research

The purpose of this study is to apply the concept of CPTED, an environmental design for crime prevention, to cyber crime prevention. In other words, it is intended to derive cyber-CPTED countermeasures with three types of cyber-infringement: hacking, denial-of-service attack, and malicious program. In conclusion, I would like to suggest detailed countermeasures for cyber crime prevention based on the six application principles of CPTED: nature monitoring, access control, territorial reinforcement, clarity reinforcement, utility increase, and maintenance.[1][2]

1.2 The Need for Research

1.2.1 Need for CPTED

The word CPTED was started in 1971 by Ray Jeffery(Crime Prevention through Environmental)[3] to improve the residential environment, including building structures and road, to create safe zones for citizens and contribute to the pursuit of quality living in crime-free environments[4][5]. In this regard, this study will

Manuscript Received: April 27, 2021 / Revised: May 17, 2021 / Accepted: May 25, 2021
Corresponding Author: 3795879@hanmail.net
Tel:+82-031-450-5161
Professor, Dept. of Liberal Arts, Hansei Univ., Korea

combine the concept of CPTED, a crime prevention through improving the physical environment, into the cyber environment to find a crime prevention measure through the design of a cyber environment.[6]

1.2.2 Features and Severity of Cybercrime

Cybercrime has the following characteristics. First, it is anonymity and non-face-to-face. Crimes occur without face-to-face interaction between the parties and are highly likely to occur repeatedly. Second, it is wide area and professional technicality. No geographic or spatial limitations, so there is a huge international impact. Third, potential and spread. It is difficult for victims or investigative agencies to identify, it is difficult to find the cause, the evidence is likely to be destroyed, and it can be extended in a short period of time. Fourth, concurrency and unlimited. In the Internet, communication can take place in real time and is not limited by space and time.[7][8]

2. MAIN SUBJECT

2.1 Prior Research

If you look at the type of research involving cybercrime prevention, table 1. As a type of cybercrime, study of the causes, and a countermeasure against, In, this type of cybercrime is internet murder, cyber finance, violence, cyber, property crime, new etc and the cause of cybercrime. Non-face-to-face, inability to, anonymity, low self-control, ethical, and measures were organized into legal defense and opportunity, good tendency, and internet ethics.

Table 1. Prior research on cybercrime prevention

category	Thesis name	Types of cybercrime	Triggering cause	Countermeasures
Lee Sung-sik (2011)	Internet ethics measures as a type-specific cause of cybercrime	Property crime, new crime cyber violence cyber violence	Criminals, penalties, cognitive insufficiency, anonymity, low self-control, and ethical	Legal action, opportunity averted, good goodness, internet ethics
Lee Sohyun Others (2019)	Feature Analysis Study by Cybercrime Type	Internet ingring, cyber financial crimes, defamation	anonymity, non-face-to-face, impulsive heart, multiple methods, multi-media use, crime incidence, unspecified crime	
Lee Yoon-ho (2011)	Daily activities and criminal damage in cyberspace	Cyber language violence damage	SNS is low and high if you play a lot of games.	Reduce game time.
		Hacking damage	Write a lot of malicious files, and the more malicious emails you distribute, the higher	Reducing malicious activity.
Kim Sang-uon Others (2012)	How to prevent cybercrime using private security	Phishing yin water flow	The more bad comments or bad emails you make, the higher it is.	Control access to key facilities such as server rooms, Fostering cyber experts,Cyber crime consulting and amendments to relevant laws
Cho Ho-dae, Shin Dong-iil (2009)	Responses to the public and private sector's analysis of cyber-invasive incidents		Policy causes and countermeasures	Maintenance and supplement of the legal system, Staffing of cyber-only investigation police, Use of external specialists of the police, activation of international co-inspectors
			Technical causes and countermeasures	Developing specialized technologies for cybercrime, Introducing a firewall system
			Environmental causes and countermeasures	Prevention activities, periodic security education, and promotional activities

2.2 The sequence of the research and the process of deriving the details

2.2.1 Order of Study

This study seeks to come up with cyber breach countermeasures in consideration of CPTED. To do this, you can use Table 2. Developed the questionnaire as analyzing the results were revised and finally proposed counter measures.

Table 2. Research Sequence

category	Questionnaire development			Questionnaire analysis			Produce results
	Draft development of questionnaire	Confirmation of questionnaire	Take a questionnaire	Reliability analysis	Investigation items	Expert opinion on factor analysis	countermeasure Suggestions for ways
Highlights	Questionnaire Pilot Development	5 investigators, security experts, etc.	29 investigators, security experts, etc.	32 items	7 items that are at the level of survey results are omitted	25 Item Factor Analysis	-
result	Detailed control items of the CPTED+ control items of ISO 27001	CPTED details (18) and ISO27001 Details (14) Confirm a total of 32 items	-	Cronbach' Alpha 0.897	Control Attractions (32□25)	Reduced to 6 inns	-

2.2.2 Questionnaire Item Development Order

The draft entry development of the questionnaire is Table 3. The items were developed in conjunction with CPTED control items and ISO 27001 control items.

Table 3. Order of development of questionnaire items

category	Confirm the type of cybercrime	CPTED Control Items	Controls in ISO 27001	Mapping between controls
Detail content	-Hacking -Service -out attack -Malicious programs	-Nature surveillance -Access control -Highly regional -High clarity -Highly usable -Maintenance	-Information Security Policy -Information security organization -Personnel security -Asset Management -Access control -Encryption -Physical and environmental security -Operational security -Communication security -System up-and-going -Supplier management -Security risk management -Business continuance management -Quasi-province	Mapping 14 controls of CPTED six application methods and information protection certification ISO 27001
content source	National Police Agency 2019 Cyber Threat Analysis Report	Crime Prevention Design Research Information Center	Controls in ISO 27001 Annex A (Annex A) of ISO27001 (2013)	Development of requirements for information security management system (ISO 27001) considering Lim heon-wook(2021) and CPTED

2.2.3 This study will investigate the types of cybercrime

In this study, we will investigate the types of cybercrime that table 4. Among the 11 types of cybercrime presented in the National Police Agency (2019 Cyber-Narrowing Analysis) we will study the causes and countermeasures for cybercrime types for hacking, service ager, and malicious programs that are guilty of violating the information and communications network.

Table 4. 11 types of cybercrime

Main Category	Information and Communications Network Infringement Crimes	Crime against the use of information and communication networks	Illegal Content Crime
Category	- Hacking - Service-out attack - Malicious programs	-Internet fraud -Cyber financial crimes -Invasion of personal location information -Cyber copyright infringement	-Cyber sexual violence -Cyber gambling -Cyber defamation and insult -Cyber stalking

source : National Police Agency 2019 Cyber Threat Analysis Report

2.2.4 Application of CPTED (Control Items)

Table 1 as a countermeasure against cybercrime. The results of the preceding study included legal treatment, opportunity prevention, good tendency, strengthening internet ethics, access control, personnel development, law-reo, maintenance, prevention activities, education, and public relations. In order to come up with a cyber breach countermeasure plan that takes CPTED into account for the purpose of this study, we will create a questionnaire in conjunction with CPTED's controls and expected countermeasures. To do this, look at the application of CPTED. The application of CPTED (or controls) is Table 5. The contents of the Crime Prevention Design Research Information Center were reorganized as follows. First, Surveillance is a way to maximize visibility and block opportunities through spatial worship and facilities to enhance natural surveillance, secondly, to enhance Access Control equipment, to control doorways and access control, and third, territory reinforcement to display boundaries, strengthen ethics, and strengthen legal penalties. Fourth, The Legibility Reinforcement is to enhance symbolism, enhance color, and prohibit reproduction by utilizing promotional products. Fifth, Activity Support is to explore utilization, increase utilization through short haired events, and increase surveillance through manned periodic events. Sixth, Maintenance & Management includes image and security education, and good tendencies.[9][10]

Table 5. 6 Application Reasons and Applications for CPTED

Application rules	Small class	content
1.Surveillance	-Increased visibility	Maximize visibility through road structures and building buildings
	-Stronger natural senses	Monitoring of natural intrusions through space storage and facility design
	-Block opportunities	Blocking access to certain boundaries, such as fences
2.Access Control	-Equipment stronger	Prevent crime directly through security facilities
	-Doorway control	Access control to induce certain spaces such as roads, walkways, landscaping, doors, etc.
	-Restricted traffic time	Restricted access time from the access control system
3.Territoriality Reinforcement	-Borderline display	Mark boundaries so that you can assert the private rights of a specific target
	-Ethical becoming stronger	Building areas separated by public and private areas through India and landscaping
	-Strengthening by state	Legal tightening on penalties
4.Legibility Reinforcement	-Symbolization	Easily express signs, etc. to enhance risk perception
	-Color becoming stronger	Use color for easily recognize spaces and facilities.
	- Use prohibited publicity	Use promotional products
5. Activity Support	- Seeking ways to use	Reinforcement of play facilities and increased utilization of public places held at performances
	- manned	Increased utilization through single-channel events
	- Periodic manned	Increase surveillance opportunities by utilizing space and facilities
6. Maintenance & Management	-Image-becoming	Image-supporting image through the installation of "Crime-a-Crime Area" signs, etc.
	-Increase security education	Continuous training to ensure crime prevention is maintained
	-Good flavor	Implementation of special activities to foster good trends

Source: Reorganize the contents of the Crime prevention http://www.cpted.kr Research Information Center (1994)

2.2.5 ISO 27001 Control Items

In 1946 the International Organization for Standardization (ISO) agreed to create an integrated body at the Institute of Civil Engineering in London for international coordination of industrial standards by representatives from 25countries. 02. 23,[11] According to the Introduction of ISO27001(2013), ISO/IEC 27000 is a standard family for information protection management systems(ISO/IEC 27003, ISO/IEC 27004, ISO/IEC27005) outlines and defines information protection management systems for reference, related terms, and terms, and reference control purposes and controls in Annex A (Annex A) of ISO27001(2013) in Table 6. A total of 14 are as were classified as control items of ISO 27001.[12]

2.2.6 Similarity between CPTED and ISO27001 controls

In order to develop cyber breach countermeasures in consideration of CPTED, we were looking for similarities between CPTED and ISO27001 controls and developed questionnaires. To this end, similarity items were derived through the results related to ISO27001 and CPTED, such as Table 6.

Table 6. Technical statistics (units) related to ISO27001 and CPTED

category	(1) Security policy	(2) Information security organization	(3) Asset management	(4) Personnel security	(5) Physical and environmental security	(6)Communication and operation management	(7) Access control	(8) Maintenance of information system	(9) Security risk management	(10) Business continuity management	(11) Quasi-province	Associativity order
1.Surveillance	83				100		58					(1) Security policy (5) Physical and environmental security (7) Access control
2.Access Control	92				83		100					(1) Security policy (5) Physical and environmental security (7) Access control
3.Territoriality Reinforcement	92						58				83	(1) Security Policy (7) Access control (11) Quasi-province
4.Legibility Reinforcement	83				75						75	(1) Security policy (5) Physical and environmental security (11) Quasi-province
5. Activity Support	83				67				67			(1) Security policy (5) Physical and environmental security (9) Security incident management
6. Maintenance & Management	92							92	92			(1) Security policy (8) Maintenance of information system (9) Security risk management

Source: Lim heon-wook (2021) reconfigures the development of requirements for information security management system (ISO 27001) considering CPTED

This is a comprehensive theorem of Table 7. Similarity between the application of CPTED and the controls of ISO 27001 was derived.[13]

Table 7. CPTED application and similarity of controls in ISO 27001

Application of CPTED		Items with high similarity to ISO27001 control items	
Application rules	**Small class**	**Similar controls**	**Similar small class**
1.Surveillance	-Increased visibility -Stronger natural senses -Block opportunities	(1) Security policy (5) Physical and environmental security (7) Access control	-Security policy -Personnel security -Asset-specific rights management
2.Access Control	-Equipment stronger -Doorway control -Restricted traffic time	(1) Security policy (5) Physical and environmental security (7) Access control	-Control of entry and export of controlled areas -Network security equipment operation -Control of system access rights
3.Territoriality Reinforcement	-Borderline display -Ethical becoming stronger -Strengthening by state	(1) Security Policy (7) Access control (11) Quasi-province	-Security organization management -Security officer and operation management -Compliance with security maintenance
4.Legibility Reinforcement	-Symbolization -Color becoming stronger -Use prohibited publicity	(1) Security policy (5) Physical and environmental security (11) Quasi-province	-Compliance with information security management system -Compliance with security maintenance
5. Activity Support	-Seeking ways to use -manned -Periodic manned	(1) Security policy (5) Physical and environmental security (9) Security incident management	-Cooperation with security-related organizations -Business continuously stronger
6. Maintenance & Management	-Image-becoming -Increase security education -Good flavor	(1) Security policy (8) Maintenance of information system (9) Security risk management	-Maintenance management of security systems -Security organization management -Security response management

Source: Lim Heon-wook (2021) reconfigures the development of requirements for information security management system (ISO 27001) considering CPTED

3. RESEARCH

3.1 Research methods and contents

3.1.1 Purpose of Investigation

In an effort to use the concept of CPTED, an environmental design for crime prevention, to prevent, we want to develop cyber CPTED countermeasures with three types of cyber, service-free attacks, and malicious programs that correspond to cyber-attacks.

3.1.2 Surveyed

Investigators (12), security experts (17) CPTED and 29 experts who understand information protection certificates were interviewed using the Focus Group Interview (FGI) method.

3.1.3 Survey Details

The survey was conducted on a 5-pointscale of recurds for each, service-retas ming, and malicious program by detailed items to measure cyber breaches considering CPTED.

3.2.1 Reliability Analysis

Reliability analysis refers to the dispersion of the repeated measurements of the measurements in an analytical method representing the consistency. reliability of the measurement, the reliability measurement method is to use the Cronbach ' α (alpha) coefficient α value has a value between 0 and 1 and 0.8 or more can be a high reliability. there is the reliability of the statistical value to 0.947 as shown in the study Table 8.

Table 8. Reliability statistics

Cronbach' α (Alpha)	Number of items
0.947	96 items (32 items× types of cyber-invasive)

3.2.2 Technical Statistics

Technical statistics is a technique that summarizes the characteristics of each data as a value for the questions that are important for each of the six items for a total of 29 experts, such as table 9. Strengthening the realm strengthening penalties (4.37), clarity enhancement is information security management system compliance (4.06), increased utilization is a collaboration (4.13), maintenance security system maintenance management (4.41) was investigated as the largest value.

Table 9. Technology statistics on cyber breach countermeasures with CPTED in account

category	small Application rules		hacking	denial	malignity	average
1.Surveillance	CPTED Controls Items	Block opportunities	4.29	4.18	4.32	4.26
		Enhances natural security	3.4	3	3.33	3.24
		Increased visibility	3.5	3.15	3.61	3.42
	ISO27001 Control Items	Security policy	4.76	4.61	4.62	4.66
		Personnel security	3.46	3.36	3.64	3.49
		Manage permissions by asset	3.679	3.12	3.54	3.45
2.Access Control	CPTED Controls Items	Strengthening equipment	4.11	4.21	4.07	4.13
		gate control	2.87	2.73	2.27	2.62
		Curfew restrictions	2.54	2.08	2.25	2.29
	IISO27001 Control Items	Control of access to controlled areas	3.22	2.67	3.27	3.05
		Operation of network security equipment	4.55	4.39	4	4.31
		Controlling system access rights	4.41	3.78	4.25	4.15
3.Territoriality Reinforcement	CPTED Controls Items	High level by state	4.55	4.52	4.03	4.37
		High ethical level	4.41	4.14	4.07	4.21
		Show boundaries	2.82	2.92	3.33	3.02

	ISO27001 Control Items	Security Officer and Operations Management	4.18	4.1	3.9	4.06
		Security governance compliance	4	3.86	4	3.95
4.Legibility Reinforcement	CPTED Controls Items	Use of non-replicated promotional	2.8	2.45	2.67	2.64
		Strengthen symbolism	2.63	2.79	2.93	2.78
		Enhances color ability	2.44	2.54	2.69	2.56
	ISO27001 Control Items	Compliance with information security management system	4.04	4.13	4	4.06
5. Activity Support	CPTED Controls Items	How to use	3	3.26	3.31	3.19
		Periodic yin	3.09	3.15	3.14	3.13
		Single-haired yin	3.27	2.86	2.9	3.01
	ISO27001 Control Items	Cooperation with sheriff's organizations	4.14	4.18	4.07	4.13
		Business continuously stronger	3.45	3.32	3.66	3.48
6. Maintenance & Management	CPTED Controls Items	Increased security education	4.38	4.1	4.38	4.29
		Good flavor	2.92	2.52	2.73	2.72
		Image-becoming	2.3	2.32	2.38	2.33
	ISO27001 Control Items	Maintenance management of security systems	4.45	4.43	4.34	4.41
		Security Organization Management	4.03	3.97	4.1	4.03
		Security Response Management	4.38	4.34	4.34	4.35

3.2.3 Factor Analysis

Factor Analysis is the reduction of factors from many to a few variables through the correlation between variables. In this factor analysis, < Table 8> 32items with an average importance of less than 3points were deleted and factor analysis was performed on 25items.

How much the extracted variables are described each is represented. Table 10. is used as a result of rotating the Berry Max factor or the rotation to minimize variables with high load values of each factor to simplify factor analysis. It was summarized in six ingredients

Table 10. Rotated Component Matrix

Control items	ingredient					
	1	2	3	4	5	6
Controlling system access rights	.906	-.159	-.082	.238	.178	-.064
Operation of network security equipment	.895	.043	-.124	-.100	.215	-.033
Equipment level high	.815	-.005	.141	.284	-.126	.324
Security incident response management	.775	.391	-.189	-.251	.162	-.047
Security policy	.774	.024	.231	.214	.074	.163
Security system maintenance	.710	.172	.283	.015	.354	.071
Security governance compliance	.706	.284	.054	.022	.417	.207
Security Officer and Operation Management	.683	.230	.061	.213	.118	.574
Security Officer and Operations Management	.675	.168	.185	.157	.203	-.059
Manage your security organization	.037	.889	-.104	.214	.062	-.242
Maximize visibility	.318	.865	.121	-.166	.099	.105
Block opportunities	.137	.843	.345	.209	.031	-.032

High level of business continuity	.216	.636	.100	-.213	.576	.236
High level of personnel security	.129	-.095	.911	.000	-.116	-.004
Show boundaries	-.172	.547	.688	-.009	-.046	.118
Rights management by asset	.498	.349	.675	-.214	.089	.101
Control of access to controlled areas	-.141	.359	.669	.191	.113	.109
Compliance with information security management system	.292	-.142	.582	-.412	.304	-.080
Periodic induces	.164	-.021	-.007	.917	.031	.015
Explore how to use it	.038	.118	.032	.862	.172	.262
manned	.308	.029	-.106	.791	-.370	-.196
High level of security training	.253	.247	.136	.099	.844	.000
Collaborate with security organizations	.360	-.028	-.190	-.058	.815	.182
High level by state	.489	-.149	.459	-.143	.500	-.382
High ethical level	.327	-.387	.167	.104	.387	.689

Factor extraction method: Main factor analysis.
Rotation method: Berimax with Kaiser normalization.
a. Factor rounding converged in 15 repeat accounts.

- The first factors are system access, network security equipment, attack response, security policy, system maintenance management, security management, security management, security organization, which can be summarized as enhancing the territoriality..
- The second factor is visibility, opportunity, natural visibility, and business continuous growth, which can be summarized as natural time.
- The third case can be summarized as access control in order of strengthening personnel security, boundary line display, asset-specific rights management, control area entry and export control, and compliance with information security management system.
- The fourth key is in order of periodic benefits, utilization of the design, single-haired oil, which can be summarized as an increase in usability.
- The fifth person can be summarized by maintenance in order of security education increase, cooperation with security organizations.
- The 6th meaning can be summarized in order of punishment and ethical increase, which is the clarity.

3.2.4 Cyber breach countermeasures considering CPTED

Table 11. First, in order to enhance the importance of respondents, such as security policy training (4.66), security system maintenance management (4.41). second, opportunity protection (4.26), business continuous strengthening (3.48). third, access control is information security management system compliance (4.06), personnel security enhancement (3.49), net, In order to increase utilization, the use of defenses (3.19), periodic yin (3.13). fifth, security education training for maintenance (4.29), cooperation with security organizations (4.13). sixth, to increase area ability was derived in order to increase penalties (4.37), ethical strongness (4.21).

4. CONCLUSION

4.1 Research Theory

To create 32 detailed control items and derive item-specific importance in conjunction with the controls of ISO27001based on the 6 application rule of CPTED to create countermeasures that take CPTED into account to prevent cybercrime. We conducted a survey of 29 former investigators and security experts, and the results of the reliability analysis of 32 items Cronbach'α value was 0.947, the reliability of the statistical. Seven items with an average importance of less than 3 points were deleted and factored into 25 and the results were classified into six factors.

Table 11. Cyber breach countermeasures considering CPTED

category		Control items	Importance
1)factor	Legibility Reinforcement	Security Policy	4.66
		Maintenance management of security systems	4.41
		Security Response Management	4.35
		Network security equipment operation	4.31
		System access rights control	4.15
		Equipment ups and outs(c)	4.13
		Security officer and operation management	4.06
		Security Organization Management	4.03
		Security governance compliance	3.95
2)factor	Surveillance	Opportunity Blocking(c)	4.26
		Business continuously stronger	3.48
		Visibility Extreme(c)	3.42
		High level of natural monitoring(c)	3.24
3)factor	Access Control	Compliance with information security management system	4.06
		High level of personnel security	3.49
		Manage permissions by asset	3.45
		Control access to controlled areas	3.05
		Show boundary lines(c)	3.02
4)factor	Activity Support	Seeking utilization(c)	3.19
		Periodic manned(c)	3.13
		Single-haired lure(c)	3.01
5)factor	Maintenance & Management	High level of security training(c)	4.29
		Collaborate with security organizations	4.13
6)factor	Territoriality Reinforcemen	Level high by state(c)	4.37
		High ethical leve (c)	4.21

※ (c) CPTED control items

If you propose two typical measures. first, we propose natural monitoring opportunity blocking, business continuous stability strengthening measures to maximize visibility and block opportunities through space storage and facilities. second, access control to strengthen equipment and control entrances to and from the information security management system. Proposing ways to strengthen people's security. third, displaying boundaries, strengthening ethics, strengthening legal penalties, proposing ways to strengthen penalties, strengthening ethics, strengthening the fourth, symbolism, color-ability, and enhancing readability such as avoiding reproduction utilizing promotional materials, proposing security policy management measures. fifth, increasing utilization to enhance guidance and monitoring through events, and more Proposes periodic

guidance. and sixth, proposes security education, collaboration with security-related organizations for maintenance such as image and security education, and good trends.

4.2 Expected Effects

The differentiator of this study is Table 1. Prior research has approached types of cybercrime such as cyber violence, Internet fraud, cyber finance crimes, defamation, the use of phishing scams, which are among table 4.11 types of cybercrime, and are subject to information and communications network use crimes and illegal content crimes. and the cause of this is a lack of penalties, If you want to find the cause in the psychological phenomenon of individuals such as low self-control, anonymity, this study approached the crime type as an information and communication network infringement crime corresponding to information protection. and the causes and countermeasures accordingly were also tried to find countermeasures through the control items of ISO27001 corresponding to CPTED and information protection corresponding to physical security. In other words, we have tried to find countermeasures against cybercrime in psychological areas, but this study is discriminatory that we have approached to find in cyber countermeasures. This has led to a wide range of approaches to solving cybercrime in the future.

4.3 Limitations of research

The purpose of this study is to bring the concept of physical CPTED into cyber concepts. and its attempts have been limited from the beginning, resulting in natural sense of opportunity and continuous business Access control is management system compliance. and personnel security, area strengthening is to strengthen the penalties and strengthen the ethical readability is security policy training and security system maintenance management, utilization increase is a means of seeking utilization. and periodic guidance, maintenance was this countermeasures. such as strengthening security education and security-related organizations. but derived results based on surveys for professionals. There was a limit to linking and deriving physical measures and cyber measures.

REFERENCES

[1] H. W. Lim, “Security education and research in accordance with the paradigm shift in the industry Security,” *Journal of Security Engineering,* Vol. 12, No. 6, pp. 597-608. 2015.

[2] H. W. Lim, “Security-equipment building cause based on「grounded theory」approaches.” *Journal of convergence security.* Vol. 16, No. 7, pp. 69-75. 2016.

[3] Y. G. Kang, & M. Y. Park, “A Study on the Legislation to Systematize CPTED”, *The Journal of Police Science*. Vol. 14, No. 2, pp. 3-28. 2014

[4] J. I. Choi, S. C. Park, H. J. Choi, & H. W. Park, “Development of the Design Evaluation Model for School Facilities Crime Prevention”, *THE JOURNAL OF KOREAN EDUCATION,* Vol. 40, No. 3, pp. 133-154. 2013.

[5] H. W. Lim, “Business model correlation analysis according to the technology maturity of the information security industry”, *Journal of convergence security*, Vol. 19, No. 4, pp. 165-171. 2019.

[6] National Police Agency. Crime Prevention (CPTED) Plan through Environmental Design. *Department of Life Safety*, 2005.

[7] H. D. Cho, “The Investigation Professionalization Korean Police at Cyber Crime”. *The Korean Association of Police Science Review*, Vol. 13, No. 5, pp. 239-258. 2011.

[8] H. D. Cho, & D. I. Shin, “Countermeasure by Cyber Infringement Accident Present Condition Analysis of Public and Private Section”. *The Journal of the Korea Contents Association*, Vol. 9, No. 1, pp. 331-338. 2009.

[9] H. W. Lim, “Developing the requirements of National Important Facilities according to the certification criteria of (ISO)”, *Journal of convergence security*. Vol. 17, No. 3, pp. 65-71. 2017.

[10] H. W. Lim, "Marketing strategies of Information security management system". *Journal of Security Engineering*. 12. Vol. 12, No. 4, pp. 305-318. 2015.
[11] H. W. Lim, "Development of requirements for information security management system (ISO 27001) with CPTED in account", *Journal of Security Engineering*, Vol. 21, No. 1, pp. 19-24. 2021.
[12] http://www.cpted.kr. Criminal Prevention Design Research Information Center
[13] https://www.kab.or.kr/