A Research on Security Education Framework for Employee's Behavior Change

Kunwoo Kim, Myeong-Gyun Song, and Jungduk Kim

***Abstract*—The development of information technology has a positive impact on business environment and at the same time, a negative impact on various security threats. Organizations try to implement various countermeasures for preventing security incident. However they tend to rely on technical security solution and security incidents are not possible to prevent completely. Recently, People Centric Security as a new approach has become an issue and the security education for changing the behavior of employees is emphasized. However, most organizations have difficulty in expecting any changes in behavior of employees because security education regards as a formal activity for compliance. Moreover, few previous security education-related researches studied the relevance of the educational contents necessary for employees with the behavioral changes in students and security experts. The purpose of this research is to provide security education framework for employee's behavior change based on pedagogy and social psychology. In addition, some future researches that overcome the limitation of this research for effective security education program were proposed.**

***Index Terms*—Security education, social psychology, people centric security.**

I. Introduction

Today, the rapid development of information technology has greatly contributed to improving organizational work productivity. However, threats like APT (Advanced Persistent Threat) appeared and internal information leakage paths became diversified. For this reason, small and big security incidents are occurring every year. Statistics showed that the scale of security industry is increasing continuously and most organizations rely highly on technical security solutions [1]. However, security incident is caused by a human being who lacks security consciousness and it is also the human who solves this problem. If security is not supported by the security awareness and capability of individual organizational members, it is of no use.

Gartner proposed a new paradigm of human-centered security [2]. Human-centered security is an approach to assign responsibility and authority based on trust in employees, improve security awareness and capability through education, and detect and respond to abnormal symptoms quickly through continuous monitoring. In other words, the approach is to improve the security awareness by carrying out security education continuously from the point of employment of employees and the security capability of individuals for preventing and responding to security incidents.

However, it will not be effective unless the security education remains temporary and the behavior of employees is improved. Most organizations perform minimum security education depending on compliance. Furthermore, to look at the recent trends of security education studies, most studies related to security education in Korea are largely on methods to cultivate security personnel, security education courses in institutions and universities, and impact of security education on security policy observation and few studies deal with educational contents [3].

This research aims to look at the concept of education based on pedagogy and social psychology, understand influential factors to human behavior and methods to change behavior, and provide the framework for security education containing security education contents necessary for behavioral changes in employees. It also describes methods to perform education depending on the framework and proposes future research tasks for developing effective education programs.

Manuscript received December 5, 2016; revised April 3, 2017.

Kunwoo Kim, Myeong-Gyun Song, and Jungduk Kim are with the Department of Security Convergence, Graduate School of Chung-Ang University, Seoul, Republic of Korea (e-mail: kunwoo.kim317@gmail.com, a50692911@gmail.com, jdkimcau@gmail.com).

II. Related Work

A. Concept of Education

To define the term education exactly, it is necessary to look at the nature of education based on the origin of word. To look at the origin of word 'education,' the term's verb form 'educate' derived from 'educare' in Latin and this can be interpreted that 'e' indicating 'out' and 'ducare' indicating 'to lead' are combined to represent 'to lead out' [4]. In other words, this suggests that acquiring knowledge is important, but putting this into action is also important.

To define education from the theoretical perspective, education is defined largely into two aspects in pedagogy. First, education means passing on something valuable to those who are educated so that they can commit themselves to the field they belong to in the future and focuses on cognitive changes [4]. Second, education is a process to change human behavior intentionally and emphasizes behavioral changes [4]. In other words, education is a process to acquire and practice standard of judgment and knowledge that ought to be followed when a human being behaves and judges. Here, the word 'intentionally' indicates educational program, which consists of educational contents, methods, and evaluations. Educational contents can depend on educational field or course, but the selection criteria for general educational contents commonly require consistency with goals, breadth and width of required knowledge, and

doi: 10.18178/ijiet.2018.8.1.1014

practicability.

To look at the educational method, there are lecture method, discussion method, and questioning method and it may depend on educational contents [5]. Lecture method is a method that individuals or groups who have more knowledge convey knowledge to those who have less knowledge. Discussion method is a method that those who are subject to education participate voluntarily, discover problems on a particular subject, and explore solutions. Questioning method is a method that educators encourage those who are subject to education to draw inference and acquire knowledge by asking questions.

Finally, the term educational evaluation can be defined as a process to collect and use the behavioral changes of those who are subject to education and the educational courses to determine the achievement of educational goal and the efficiency and effectiveness of educational course and then make educational decision making [5]. Evaluation method can be classified into diagnostic evaluation, formative evaluation, and summative evaluation, and with the recent evolution of diagnostic evaluation and formative evaluation in terms of concept and description, such cases that perform all three forms of evaluation are increasing.

B. Influence Factors to Behavior and How to Change Behavior

This section identifies the influential factors to human behavior from social psychological aspects to draw the framework for security education for behavioral changes of employees and describes methods for changing behavior. In the first place, a process until a particular behavior is executed can be explained by the Cognitive Information Processing Theory that regards human thinking process similarly to computer information processing process and the Theory of Planned Behavior, a representative theory on psychological characteristics and behaviors in social psychological field. Cognitive Information Processing Theory is executed by passing through attention, perception, representation of human behavior, comparison with the existing information, and meaning-imparting stages [6]. According to this theory, in order to change human behavior, messages to deliver should be exposed and perceived by paying attention to them and positive intention should be formed.

On the other hand, Theory of Planned Behavior explains the influential factors to human behavior that are determined by intention and influences intention with attitude, subjective norm, and perceived behavior control [7]. Attitude is a concept that encompasses both cognitive judgment and emotion toward a particular object and indicates favorable or unfavorable evaluation of an object. To elicit changes in behavior, employees should be exposed to the messages that can be attended or concentrated, as shown in Cognitive Information Processing Theory [8]. To solve these problems, they should be encouraged or persuaded to understand what to do and staffs should be made to accept these [9]. Finally, methods to maintain a positive attitude should be provided so that executives can accept [8].

Subjective norm means an evaluation of people around especially of the behavior of an individual including self-evaluation of behavior. It is a determination of whether to behave or not by comparing other's behavior with one's belief. In other words, it is influenced by social learning [10]. Subjective norm also means social pressure indicating that individuals feel in making a decision about whether to behave or not [10]. One's behavior is suppressed by such social pressure.

Perceived behavior control means a degree that one perceives ability and confidence required for doing an act. This perceived behavior control can be strengthened by reinforcing the self-efficacy that indicates that one is motivated before putting into action and evaluates by oneself regarding a particular ability [10]. On one hand, if one does an inappropriate behavior or unless one performs an act that is required, attribution error, which indicates that one ascribes negative results to somebody else, might occur [11]. Influential factors to behavior as shown above and social psychological methods to change and reinforce this can be summarized in "Table I".

TABLE I: INFLUENCE FACTOR TO BEHAVIOR AND HOW TO CHANGE AND STRENGTHEN FACTOR

Influence factor to behavior	*Attitude*	*Subjective norms*	*Perceived behavior control*
How to change and strengthen factor	Attention Exposure Comprehension Persuasion Acceptance Retention	Social Learning Social Pressure	Motivation Attribution Self-Efficiency

C. Security Education

To look at the definition of security education for employees, Michael E. Whitman and Herbert J. Mattord defined security education as part of security program, specifically as activity to reduce security incident that occurred due to lack of awareness among employees [12]. On the other hand, Wilson and Harsh defined security education as a process that employees acquire knowledge and technology to perform security activity in preparation for new technologies and threats that might happen [13]. In other words, security education can be defined as an "activity to acquire and practice knowledge on security activities that are required on business in order to prevent and respond to the security incident that are caused by technological change and new threats and intended or unintended behaviors of employees."

The existing security education related studies were mostly the fragmentary ones that provided codes of conduct for a particular situation and lacked security research contents from comprehensive aspects [3]. Therefore this section aims to deal with the requirements for information security certification and the security education related contents that must be recognized and practiced by employees. The control area for Information Security Management System (ISMS) Certification in Korea includes security control related to security education. Such information includes five fields: overview of security, security policy and regulation, security incident case and countermeasure, security related law, and responsibility for violation of regulation. Although these are recommended to be taught, these five fields do not have

specific educational contents. For this reason, this research identifies some security controls as educational contents related to the role and responsibility to be performed by employees. These security educational contents to reinforce the security activities of employees in five educational fields can be summarized in "Table II."

TABLE II: SECURITY EDUCATION FIELDS AND CONTENTS

No.	*Field*	*Content*
1	Overview of security	definition and necessity of security, latest security threat and vulnerability
2	Security incident case and countermeasure	Security incident cases (including other companies), security incident training, security incident report
3	Security policy and regulation	organizational security policy and regulation, security requirement at contract, implementation of supplier security management, security requirement at termination of contract, information assets identification, security level assignment, handling procedure, education execution and evaluation, security at the time of retirement and job change, secure area, access control, surveillance, information assets (mobile) carry-in and carry-out, personal work environment security, public work environment security, security system, smart work security, information transmission policy, removal device management, malicious code control, access and use monitoring
4	Security related law	laws on the industrial field which an organization belongs to, security related laws including privacy act
5	Responsibility for violation of regulation	confidentiality agreement, reward and punishment regulation

III. SECURITY EDUCATION FRAMEWORK

The framework for security education that contains the influential factors to behaviors identified in previous studies and the social psychological methods for behavioral changes in employees depending on security education contents is shown in "Fig. 1". Educational contents in five fields all have relevance to attitude, subjective norm, and perceived behavior control and the detailed educational contents are classified by factor.

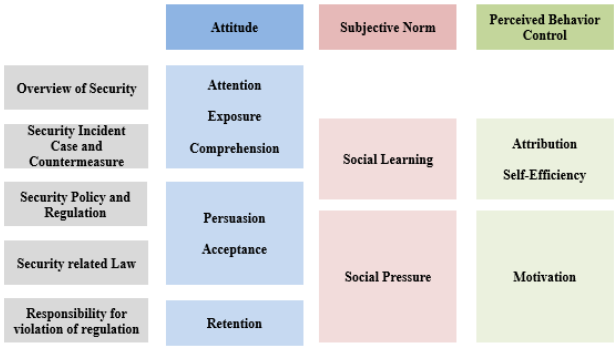

Fig. 1. Security education framework.

A. Education for Attitude Changes

At the first, prior to security education, employees' attention must be attracted by explaining about the security threats that have become an issue and the security incident cases. At this time, employees should be encouraged to understand the importance and necessity of security by explaining about an organization's past incident cases and other organizations' cases. And they can be more persuaded by explaining about the damages and disadvantages that might occur in case not observing the security activity and procedure required in security policies and regulations. In particular, the width of acceptance can be widened by communicating that an organization's security policy and regulation is a requirement of the laws related to organizations. Finally, the awareness of security activity can be improved and the security activity can be maintained by explaining about legal liability and requesting confidentiality agreement. Therefore, the following items should be included in security education.

- Overview of security: latest security threats and vulnerability, definition and necessity of security
- Security incident case and countermeasure: security incident case
- Security policy and regulation: construction of organizational security policy and regulation, security requirement at contract, implementation of supplier security management, security requirement at termination of contract, information assets identification and security level assignment methods and handling procedures, security at the time of retirement and job change, secure area, access control procedure, surveillance, information assets carry-in and carry-out procedure, personal/public work environment security, smart work security, information transmission policy, removal device management, malicious code control
- Security related law: laws on the industrial field which an organization belongs to, security related laws including privacy act
- Responsibility for violation of regulation: confidentiality agreement, reward and punishment regulation

B. Education for Strenghtening Subjective Norms

If we recognize the concept and importance of security and then compare the suggestions of security incident cases happened in other organizations with the security activities required by the organization that employees belong to will bring about a positive learning effect. In addition, if we recognize that security education is followed by evaluation and the results are reflected into the employee performance rating, it will bring about a learning effect. On the other hand, if we recognize that the behavior of employees is monitored and the nonobservance of related laws and regulations leads to disadvantages, it will be helpful for suppressing malicious behaviors as a kind of social pressure. Therefore, the following items should be included in security education.

- Security incident case and countermeasures: security incident case
- Security policy and regulation: education execution and evaluation, surveillance, access and use monitoring
- Security related law: laws in the industrial field that an organization belongs to, security related laws including privacy act
- Responsibility for violation of regulation: reward and punishment regulation

C. Education for Strenghtening the Perceived Behavior Control

In general, humans tend to ascribe negative results of

behavior to someone else. To prevent this attribution error among employees, there is a need to inform inappropriate behaviors that might occur while working. On the other hand, it is also necessary to improve self-efficacy by communicating that security activity can be performed smoothly according to the security regulation of an organization. Also, if they are motivated to recognize reward and disciplinary action as result of security activity, it may have a positive effect on compliance with policies and regulations. Therefore, the following items should be included in security education.

- Security incident case and countermeasure: participation in security incident training, security incident reporting procedure
- Security policy and regulation: security requirement at contract, implementation of supplier security management, security requirement at termination of contract, information assets identification and security level assignment methods and handling procedures security at the time of retirement and job change, secure area access control procedure, information assets carry-in and carry-out procedure, personal/public work environment security, smart work security, information transmission policy, removal device management, malicious code control, access and use monitoring
- Security related law: laws in the industrial field that an organization belongs to, security related laws including privacy act
- Responsibility for violation of regulation: reward and punishment regulation

IV. Future Research

This research is the one that draws the security education framework for explaining about the relevance of influential factors to human behavior from social psychological aspects and methods for behavioral changes to security education contents and focuses on security education contents for behavioral changes in employees. Therefore, the effective security education performance tasks that are based on the suggestions of the previous studies are proposed as future research tasks because such items as educational method and evaluation one, among many constituents of education are not included.

First, it is necessary to test the reliability and validity of the framework proposed in this research. Second, it is necessary to carry out additional studies on educational methods depending on educational contents. Third, it is necessary to conduct a research on the development of evaluation items to measure the behavioral changes of employees. Finally, it is necessary to conduct a research on the development of effective e-learning contents and evaluation methods because there are limitations in educating all employees at the same time and place and repeating such education. If we carry out a research on on/offline educational contents, methods, evaluation methods, and effectiveness like above, we will be able to understand human behavior more closely and contribute to theory and practice.

V. Conclusion

At security related seminars or conferences, it is quite often heard that 'security is all about people.' This means that the cause of security incident is people and it is also the people who solves it. However, it is true that organization's security measures today relies highly on technical solutions and the security education for improving the awareness of security for employees and enhancing their capability is the minimum activity for compliance. This suggests that education simply delivers knowledge in most cases and neglects behavioral changes, although the purpose of education is to convey knowledge and seek behavioral changes. Moreover, we still have few security education related studies for employees and especially lack of studies on security education contents. Therefore, it is necessary to conduct a study on security education contents that must be recognized by considering the behavioral changes of employees in order to establish and perform effective security education programs in an organization.

This research proposed the security education framework for behavioral changes among employees based on pedagogy and social psychology and drew security education contents necessary for employees by considering the relevance of five educational fields to the factors to reinforce changes in attitude, subjective norm, and perceived behavior control. This research is significant in that it provided a comprehensive framework for the relevance of human behavior to security education contents under the current situation that we still have few studies on security education in Korea. However, this research is an exploratory one for drawing a framework and thus has limitations in that it is difficult to generalize because the reliability and validity of the framework was not tested and that it did not include security education performance method and evaluation method. Therefore, to overcome such limitations of this research and establish effective security education programs, it is necessary to conduct a research on measurement of effectiveness of security education, educational performance method and evaluation method depending on educational contents, how to measure behavioral changes, and online educational program development and its effectiveness measurement.

Acknowledgment

The This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2016-H8501-16-1018)) supervised by the IITP(Institute for Information & communications Technology Promotion)

References

[1] R. Contu, C. Canales, and L. Pingree, *Forecast: Information Security Worldwide 2012-2018*, Gartner, G00264279, 2014.
[2] T. Scholtz, People Centric Security Strategy, Gartner, G00249357, 2013.
[3] K. Kim and J. Kim, "An analysis of research trends in information security education," *Journal of The Korea Institute of information Security & Cryptology*, vol. 26, pp. 489-499, April 2016.
[4] R. S. Peter, *Ethics and Education*, London: Georg Allen and Unwin Ltd., 1966.
[5] J. S. Bruner, *The Process of Education*, Harvard Univ. Press, 1960.
[6] A. Searleman, and D. Hermann, *Memory from a Broader Perspective*, McGraw-Hill, 1994.

[7] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179-211, December 1991.
[8] P. G. Zimbardo and M. R. Leippe, *The Psychology of Attitude Change and Social Influence*, McGraw-Hill, 1991.
[9] J. Greenberg, and R. A. Baron, *Behavior in Organizations*, Allyn and Bacon, 1993.
[10] A. Bandura, *Social Learning and Personality Development*, Holt, Rinehart, and Winston, 1963.
[11] C. Roper, L. Fische, and J. A. Grau, *Security Education, Awareness and Training: From Theory to Practice*, Butterworth-Heinemann, 2005.
[12] M. E. Whitman and H. J. Mattord, *Management of Information Security*, Thomson Course Technology, 2004.
[13] M. Wilson and J. Hash, *Building an Information Technology Security Awareness and Training Program*, NIST Special Publication 800-50, 2003.

Kunwoo Kim was born in republic of Korea in 1981. He got the bachelor's degree in 2008 majored in information systems, the master's degree in 2010 majored in information security and system audit from Chung-Ang University in Republic of Korea. He has a work experience with security consultant at A3 security and worked for Hyundai Mobis as an enterprise security manager. He currently is the Ph. D. candidate in Chung-Ang University. His research interests include people centric security, information security management, information security governance and cyber resilience.

Myeong-Gyun Song was born in republic of Korea in 1990. He got the bachelor's degree in 2015 majored in information systems. Currently he is studying security convergence on his master's degree course in Chung-Ang University. His research interests include information security management, information security governance, security culture and cyber resilience.

Jungduk Kim was born in republic of Korea in 1956. He got the bachelor's degree in 1979, the master's degree in 1981 from Yonsei University in Republic of Korea. He also got the MBA from University of South Carolina in 1986 and the Ph.D. from Texas A&M University in 1990 majored in MIS (management information systems).

He has researched in information system and security as a professor in Chung-Ang University and currently he is a professor at the Department of Industrial Security. He has lots of experiences in ISO/IEC JTC1 SC27 and he participated in international standardization activity in ISO/IEC 27014(Governance of Information Security) as an editor from 2010 to 2013. He is engaged in various research activities at academic institutions such as KIISC(Korea Institute of information Security & Cryptology), KMIS(The Korea Society of Management Information Systems), KAIS(The Korea Association for Industrial Security) and so on.

His current research interests include people centric security, information security management, information security governance, cyber resilience, digital business security, usable security, security analytics and economics of security.