IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 2, February 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

# A Study on Risk Management in Digital Risk Society

**Ji-Yeon YOO**

Department of Information and Security Management
Sangmyung University
Seoul City 03016, Republic of Korea

**Abstract**

As the information society becomes further dependent on IT, the security risks are also expanding as a whole and its seriousness is increasing to a level that cannot be neglected.

From that point of view, this study examines the incidents of damage caused by digital accidents and the risks in the new environment. In order to elucidate the advancements of digitalization and conceptualize digital disasters, I would like to draw policy implications for forecasting and responding to future potential digital disasters.

Keywords: *Digital Technologies, New Field of Risk Inquiry, Digital Risk Society, Digital Social Inequality Risks, Risk Management*

## 1. Introduction

As the digital society becomes more sophisticated, more time is spent in environments controlled by technology, and as the dependence on technology increases, the digital environment becomes larger and more complex. The increase in complexity is inversely proportional to the trust of technology, which means that the technical system is likely to produce erroneous outcomes. Here is the dilemma of information society development. And the dilemma of digital society development is expected to deepen as it progresses to the Hyper-Connected Society, where the society as a whole converges digitally. Second, a connected society increases the likelihood of information disclosure, system malfunction, improper access, and unpredictable risks as all objects are digitized and connected with human systems.

In this study, we define the term digital risk society as the deepened risks to society caused by the progress of the digital convergence of society. Digital danger society is a society in which the risk of information technology as a social infrastructure is expanded and reproduced throughout the social system as a whole. The boundaries between the virtual space and the physical space are digitized, and the virtual space and the physical space are exposed in its complexity. The expansion into digital convergence produces two characteristics of the digital risk society. Maximizing the risk through the network, and increasing the risk to the physical space, the virtual space, and the hybrid space.

## 2. Digital Risk Management Theory

Risk management refers to all regulatory actions intended to affect the development and response of [1][1].

In other words, risk management is a multi-faceted process that consists of various aspects and continues to be repeated. Thus, the scope of risk management expands from risk prediction to prevention, and specifically, it includes risk perception or identification, risk assessment, control and mitigation, and risk communication[2].

In general, the risk management model is divided into preventive, preparedness, response, and recovery. Prevention and preparation based on time can be classified into pre-activities, while responses and restoration can be classified into post-activities. Prevention is an activity that evaluates the actual risks or potential risks, and reduces the risks. Contrast refers to the development of response plans based on risk assessment, training of response personnel, preparation of necessary resources, and clarification of responsibilities. Responses include enforcement of the plan, reduction of the possibility of secondary damage, and preparation for the recovery phase. The restoration refers to the reconstruction of the system, such as support until returning to a normal state[2].

Table 1: Steps and Content of Risk Management

| Step | Functions | Main Content |
|---|---|---|
| Prevention | Understand and predict | Activities that generate understanding, prediction and communication information about risk |
| | Identify and remove risk sources | Analyze the data collected through the research results and monitoring activities by the type of risk, and remove the risk factors for each |

[1] Similarly, Cutter (1993) defines hazard management as activities that help generate awareness of the hazards, make decisions about them, and put appropriate controls or mitigation strategies into action accordingly.

| Step | Functions | Main Content |
|---|---|---|
| | | institution |
| | Gather and evaluate risk information | Activities that collect, analyze, and report information about risk situations to provide information needed for key decisions |
| Prepare | Establish advance measures | Activities that coordinate and cooperate with each other in the risk management field, taking into consideration the feasibility, effectiveness, and promptness before risk occurrence |
| | Maintain risk management ability | Current risk management capacity, i.e. activities that assess and sustain resources that can be used for actual risk |
| Respond | Enforcement of measures | Activities that actually perform the measures already established when the risk becomes reality |
| | Emergency recovery | Continuously support activities until the damage caused by the risk returns to normal |
| Restore | Mid-to-long term recovery | Activities that continue to support the damage from its initial recovery period until it returns to normal |
| | Assessment and improvement | After the implementation of the measures, evaluate and learn the causes and activities throughout the course, analyzing the problems and finding improvement plans |

Source: Sung, et al., 2007[2]

This risk management applies to all risk types. Depending on the type of risk, the cause and nature of the problem vary. So different risk management strategies and counter measures are needed depending on the nature and circumstances of the risk. Here, the existing risk management and the risk management in the new environment are examined using the three-dimensional structure of the cause, object, and space of risk.

## 3. Structuring Risk Management

Existing risk management, as shown in Figure 1, basically tends to be done by risk factor in terms of elimination and reduction of risk factors. Risk space is classified into physical space and virtual space, and risk causes are classified into natural, social, and technical causes. Natural hazards in physical space are marked by a single point, and when a new dimension of hazardous objects is added to them, individual, social, and national risks are represented by their respective points.

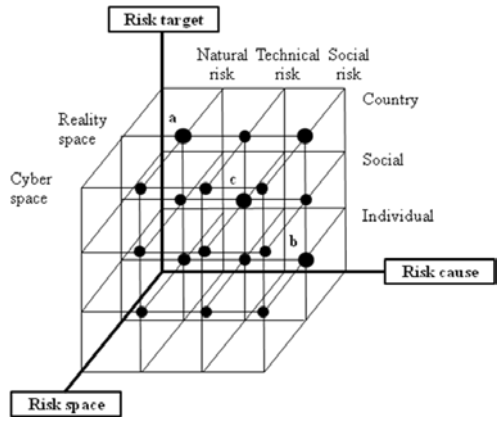


Figure 1 Existing Risk Management

Natural hazards are difficult to completely eliminate, but they are managed to prevent disasters at the national level, such as the reconstruction of dams to minimize flood damage and disaster recovery. Floods, which area representative example of natural risk based on national physical space, are managed by the National Emergency Management Agency. The Ministry of Land, Transport, and Maritime Affairs is in charge of flood and disaster prevention facilities. In the case of floods in the Imjin River basin in July 1999, the National Emergency Management Agency (NEMA) responded to the disaster and attempted recovery of the municipality with the Ministry of Land, Transport, and Maritime Affairs(see Figure 1).

Social risk is managed by national, social, and individual management activities such as ethics education, community patrols, and the criminal justice system in order to maintain public order. Crime, which is a representative example of social risk based on the physical space at the individual level, is handled with risk management approaches in order to enforce the rule of law and to secure public safety. In the case of the disappearance of the "frog boys" in 1991, the police made an investigation and led a rescue effort (see b in Figure 1).

Technical risks are managed at the national, enterprise and social level, such as the technical safety certification system, education and training, technology development and technological advancement in order to minimize the damage caused by system failure. However, risk management for the prevention of these technical risks may result in new, complex technical risks. Gas explosions, which area representative example of technical risk based on the physical dimension of the social dimension, are managed by enterprises and the local government through the industrial safety management system. In the case of a gas explosion in the Daegu subway in April 1995, the National Emergency Management Agency (NEMA)

responded to the disaster and initiated a recovery effort with the local government (see c in Figure 1).
This risk management is carried out with a risk paradigm such as the complexity of risk occurrence and uncertainty as a risk response. In other words, rather than risk management after an event has occurred, risk is managed to prevent the disaster from happening.

## 4. Structuring Digital Risk Management

However, in the digital risk society where the risks are intermixed, the risk cause, the risk object, and the risk space are combined, and as shown in Figure 2 the sea remixed and not overlapping. As a result, risk management becomes difficult and new countermeasures are required. That is, when the cause of the risk is simple and the risk object and scope are limited, risk management is performed by eliminating or reducing the risk factors. However, it is difficult to manage the risk on a one-to-one basis.

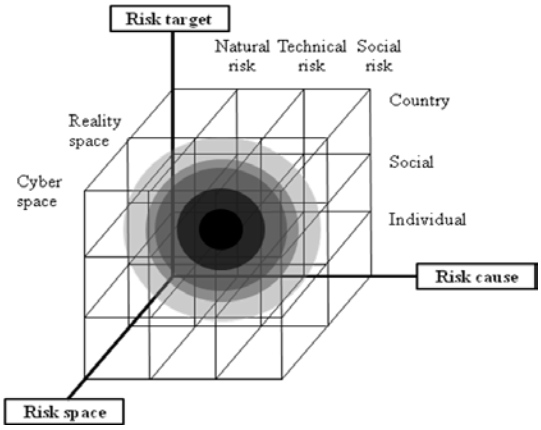


Figure 2 Risk management of digital risk society

In particular, the government is making urgent efforts to prepare for disasters characterized by unpredictability and uncertainty. The digital risk society is networked, so problems arising in a specific transaction can occur instantaneously or at different times in different places. Aproblem in a specific place is not assumed to be solved simultaneously in other places connected to it[3][4][5]. Therefore, it is necessary to establish an integrated preventive, preliminary, response and recovery system that can prepare for unexpected accidents or disasters and institutionalize a public mechanism that disperses the risks.
For example, if a malicious code is installed in the central control system of a main infrastructure control system, then all the traffic flow in Korea can be controlled by the cyber attacker. When a traffic light changes from go (green) to a sudden stop (red) as the cyber attacker intends, traffic on the road will collide. It is not so difficult to inject malicious code with either a personal vehicle system connected to a traffic control central system; a personal smartphone connected to a personal vehicle system; or a personal smartphone via a personal smartphone.
Unexpected risks arise in the physical space and the virtual space. In order to solve such a risk problem, risk management policies and countermeasures must be simultaneously performed in the physical space and the virtual space.
In short, with the new risk paradigm shift, risk management in the digital risk society requires an integrated and organic structure as shown in Figure 2. Digital risks require new risk management strategies because information technology and networks operate on a social basis, are complex and networked, and risk is likely to expand and reproduce.
In this study, we define risk management concepts with the term Digital Risk Management. Digital risk management refers to the entire process of integrally recognizing, evaluating, controlling, and preventing the technical risks of the society as a whole in the physical space and the virtual space.
The conceptualization of digital risk management is meaningful for expanding the discussion about the technical dimensions from the information society perspective[1].
Information security means a series of efforts to protect information, systems and services from the mistakes of the users of the system, including mechanical errors and illegal manipulation, thereby minimizing the possibility and impact of the accident. In particular, the purpose of information security is to ensure the confidentiality, integrity and availability of information and systems by taking measures that can eliminate serious threats or reduce them to an acceptable level.
In other words, information security protects against illicit exposure, tampering, and destruction by intentional or accidental oversampling, processing, storage and transmission of information in the system or electronic form, so that legitimate users can access the desired information easily and quickly. Information security is used to maintain the confidentiality, integrity and availability of information[6][7] [2]. This means that it

[1] The information security presented in the solution process of the dysfunction to the technical social level by approaching from the risk management view

[2] Organization for Economic Cooperation and Development (OECD), Guidelines for the Security of Information Systems, 1992 (http: // www .oecd.org / document / 19/0, 2340, en_2649_34255_1815059_119820_1_1_1, 00.html)
The objective of security of information systems is to protect the interests of those relying on information systems from harm resulting

protects against the illegal intrusion by a malicious third party, information leak or system destruction in a space connected via a network such as the Internet[1].

## 5. Conclusion

This approach to information security from a risk management perspective has several implications[8]. Above all, the issue of information security goes beyond the level of recognition as mechanical error or system destruction, providing a basis for social and national problems. In other words, it can take digital risk as a problem of social areas as well as technical response measures, and raise awareness of roles, duties and responsibilities at the individual, social and national level.
It is also possible to re-examine the issue of information security through theories discussed in traditional risk studies. For example, risk is divided into objective or statistical risk, subjective or perceived risk, and effective risk[8][9][10]. The policy implications of this conceptual distinction can be found in risk identification or identification, risk assessment, control and mitigation, and risk communication as presented in the risk management process. In information security, security experts and policy makers have determined the process of risk management based on the objective risk based on security factors and rules. However, in terms of digital risk management, the risk process should be analyzed and evaluated based on subjective and actual risks.

## References

[1] Hood, C. and Jones, K.C. "Accident and Design: Contemporary Debates in Risk Management". UCL Press. 1996.
[2] Sung, J., Jung, B., and Song, W. "Technology Risk Management in a De-Pursuing Innovation System", Policy Research Institute for Science and Technology Policy 2007-17-2. 2007.
[3] Perrow, C. "Normal Accidents: Living with High-Risk Technology". Basic Books. 1984.
[4] Kim, J. "Cyber-trend 2.0", Seoul: Jeongmundang. 2008.
[5] Kim, J. "Cyberization of Technology Risk and Privacy Right", "Social Theory," Vol. 2009.
[6] OECD "Guidelines for the Security of Information Systems". 1992. (http://www.oecd.org/ document / 19/0, 2340, en_2649_34255_1815059_119820_1_1_1, 00.html)
[7] Federal Information Security Management Act (FISMA). 2002.
[8] Chung I. "Policy Logic of Information Security as Information Society Risk Management", Proceedings of Fall 2005 Conference of Korean Public Administration Association. 2005.
[9] Slovic, P. "Perception of Risk". Science 236: 280-285. 1987
[10] So, Y., Kim, Y., Choi, B., Jung Y., and Chung I. "A Comparative Study on the Haptic Safety of Korean Nuclear Technology," Korea Atomic Energy Research Institute. 2001.

**First Author** Ji-Yeon YOO is currently a Professor of Sangmyung University. She received her Ph.D. in Information Management Engineering from Korea University. Her current research interests include Digital Risk Management, Information Strategy, and Cyber Security, etc

from failures of confidentiality, "Preservation of confidentiality, integrity and availability of information" (http://www.iso27001security.com/html/27002.html # Section2 Federal Information Security Management Act (FISMA), http://csrc.nist.gov/drivers/documents/FISMA-final.pdf; Chapter 35, Title 44 USC § 3542 (b) - (1))

[1] Weblio Dictionary Cyber Security explanation (http: / / /www.weblio.jp/content/%E3%82%B5%E3%82%A4%E3%83%90% E3%83%BC%E3%83%BB%E3%82%BB%E3%82%% AD% E3% 83% A5% E3% 83% AA% E3% 83% 86% E3% 82% A3)