Journal of Digital Convergence
Vol. 17. No. 1, pp. 141-148, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.1.141

보안 위험성향 측정을 위한 프레임워크 개발에 관한 연구

김기삼[1], 박진상[2], 김정덕[3*]
[1]중앙대학교 산업융합보안학과 석사과정, [2]중앙대학교 융합보안학과 석사과정
[3]중앙대학교 산업보안학과 교수

A Study on Developing Framework for Measuring of Security Risk Appetite

Gisam Gim[1], Jinsang Park[2], Jungduk Kim[3*]
[1]Master's Degree Student, Dept. of Industrial Convergence Security, Chung-Ang University
[2]Master's Degree Student, Dept. of Convergence Security, Chung-Ang University
[3]Professor, Dept. of Industrial Security, Chung-Ang University

요 약 디지털 기술의 발전으로 지능화 및 융합화가 가속화됨에 따라, 비즈니스 모델 및 인프라, 기술 등 여러 측면에서 기존 방식을 초월한 변화가 요구되고 있다. 변화된 비즈니스 환경에서는 다양한 보안 위험이 점증하고 있으며, 보안 위험관리의 중요성이 더욱 커지고 있다. 기존의 정보자산 기반의 위험관리에서 벗어나 비즈니스 중심의 위험관리가 대두되고 있는 시점에서 이를 위해서는 비즈니스 목표 달성을 위한 위험성향(Risk Appetite)을 파악하는 것이 필수적이며, 이는 추후 프로세스에서 발생하는 제반 의사결정 과정에 있어 판단 기준을 제공한다. 따라서 본 논문에서는 기존 위험성향 선행연구 분석 및 보호동기이론을 분석하여, 보안 위험성향 수준을 파악할 수 있는 프레임워크를 개발하였다. 또한 개발된 위험성향 프레임워크의 실무적 타당성을 검토하기 위해, 보안 위험관리 실무 전문가들로 구성된 자문위원회를 통해 적용가능성과 중요성을 검토하였다. 검토 결과, 재무, 운영, 기술, 평판, 컴플라이언스, 문화 6개의 보안 위험성향 고려 위험분야와 인지된 심각성, 인지된 취약성, 자기효능감, 반응효능감 4개의 요인이 보안 위험성향 측정을 위한 프레임워크 구성요소로서 타당한 것으로 검토되었다.

주제어 : 위험관리, 위험성향, 보안 위험성향, 위험성향 프레임워크, 위험성향 측정

Abstract The advancement of digital technology accelerates intelligence, convergence, and demands better change beyond traditional methods in all aspects of business models and technologies, infrastructure, processes, and platforms. Risk management is becoming more important because of various security risks, depending on the changing business environment and aligned to business goals is emerging from the existing information asset based risk management. For business aligned risk management, it is essential to understand the risk appetite for achieving business goals, which provides a basis for decision-making in subsequent risk management processes. In this paper, we propose a framework for analyzing the risk management framework, pre - existing risk analysis, and protection motivation theory that influences decisions on security risk management. To examine the practical feasibility of the developed risk appetite framework, we reviewed the applicability and significance of the proposed risk appetite framework through an advisory committee composed of security risk management specialists.

Key Words : Risk Management, Risk Appetite, Security Risk Appetite, Risk Appetite Framework, Risk Appetite Measurement

*This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2014-1-00636) supervised by the IITP(Institute for Information & communications Technology Promotion)
*Corresponding Author : Jungduk Kim(jdkimsac@cau.ac.kr)
Received October 30, 2018 Revised December 4, 2018
Accepted January 20, 2019 Published January 28, 2019

1. 서론

ICBM(IoT, Cloud, Big Data, Mobile)와 같은 디지털 기술의 발전은 지능화, 융합화를 가속화시키며, 비즈니스 모델, 인프라, 기술, 플랫폼 등 여러 측면에서 기존 방식을 초월한 더 진화된 변화가 요구되면서, 디지털비즈니스라는 복잡하게 얽혀있는 디지털 융합 및 복합 환경이 등장했다[1]. 이러한 변화하고 있는 비즈니스 환경에 따라 다양한 유형의 보안 위험들이 점점 증가하고 있어 보안 위험관리의 중요성이 더욱 커지고 있는 실정이다.

하지만 CISCO의 'Cyber security as a Growth Advantage' 설문조사 보고서에 따르면 기업들은 보안 위협에 대한 대비를 IT 자산 관점으로만 대응책을 마련하는 등 경영진의 위험관리에 대한 추진 노력은 크지 않는 실정이며, 대부분 기업에서는 정보시스템에 대한 취약점 점검, 모의해킹 등 취약점 관리 위주의 부분적인 위험관리를 수행하고 있다[2]. 이렇듯 기존의 위험관리는 인프라와 어플리케이션 등 IT자산에 대한 위험평가와 대책 수립에 초점이 맞추어져, 다양하고 복잡해지는 환경 변화에 대응하는데 한계가 존재하였다. 때문에 IT자산뿐만 아니라 조직의 목표, 계약상의 규정 준수 등 비즈니스와 연계된 전사적 관점의 위험관리가 수행될 필요가 있다[3].

전사적 관점의 위험관리 수행을 위해서는 비즈니스 전략 및 목표와 연계된 위험성향(Risk Appetite)의 파악이 필수적이라고 할 수가 있다. 새롭게 개정된 위험관리 국제 표준 'ISO 31000:2018' 에서는 비즈니스 목표, 운영, 전략 등 비즈니스 모든 측면에서 위험관리와의 통합을 강조했으며, 전사적 위험관리 프레임워크 'COSO ERM' 에서는 비즈니스 목표 달성을 위해 , 위험관리를 전략 및 성과와 연계하는 것의 중요성을 부각하기도 하였다. 이렇듯 보안 위험성향을 파악하는 것은 비즈니스와 연계된 전사적 관점의 보안 위험관리의 첫 내딛음으로써 수용이 가능한 위험의 수준(Acceptable Level of Security Risk)을 결정하는 것이며, 이는 추후 위험관리 프로세스에서 발생하는 의사결정에서 판단 기준을 제공한다[4].

그러나 비즈니스 목표와 연계된 위험성향 관련 연구가 미흡한 실정이며, 관련 연구가 있더라도 보안 위험관리 특성에 맞는 보안 위험성향 측정 프레임워크에 대한 연구는 미미한 실정이다. 때문에 기존 위험관리 프레임워크와 기존 위험성향 선행연구 분석, 보안 위험관리 의사결정에 영향을 미치는 보호동기 이론을 분석하여 보안 위험성향 수준을 파악할 수 있는 프레임워크 개발의 필요성이 크다고 할 수가 있다. 따라서 본 연구에서는 선행연구를 통해서 보안위험성향 측정 프레임워크 구성요소를 도출하고, 보안 위험관리 실무 전문가들로 구성된 자문위원회를 통해 적용가능성과 중요성을 검토하였다.

2. 이론적 배경 및 관련연구

2.1 보안 위험관리

2.1.1 보안 위험

위험은 조직의 자산에 발생하는 이벤트의 결과 또는 가능한 영향으로, 원치 않는 이벤트가 발생하여 손실 또는 부정적 영향을 미칠 가능성을 말한다[5] 이에 보안 위험은 사람의 실수, 또는 잘못된 행위, 지적재산권에 대한 손실, 무단 침입행위 또는 스파이, 정보탈취, 사이버위협, 절도, 소프트웨어 해킹, 자연으로 인한 재해, 서비스 품질 저하, 하드웨어 장애 및 소프트웨어 오류 및 기술적 노후화 등의 위험이 해당한다[6].

이러한 보안 위험은 디지털 기술의 발전과 함께 4차 산업혁명으로 진입하면서 보안 위험 패러다임의 전환이 일어나고 있다. 비즈니스 모델 및 기술, 인프라, 프로세스, 플랫폼 등 지능화 및 융합화가 일어남과 함께 보안위험의 유형도 복잡해지고 다양해지기 시작하였다. 이에 보안 이벤트를 완벽하게 사전에 예방하는 것은 한계가 발생하며, 디지털비즈니스 환경 내에서 위험을 효과적이고 효율적으로 관리하기 위해서는 조직의 내부의 전담부서 뿐만 아니라 관련 이해관계자를 포함하는 등 전사적인 보안이 이루어져야하는 등 비즈니스 중심의 위험관리의 중요성이 나날이 점증하고 있는 실정이다[7].

2.1.2 비즈니스 중심의 보안 위험관리

앞서 언급한 위험 패러다임 변화에 맞춰 위험관리의 패러다임도 전환되고 있다. 전통적으로 위험관리는 정보자산 및 대책 중심의 IT 관점에서의 위험관리 활동이 대부분이라고 할 수 있다. 이는 복잡해지고 다양하지는 위험 등 환경변화에 대응하는데 한계가 존재한다. 그렇기 때문에 IT자산뿐만 아니라 조직, 업무, 계약 준수 사항과 같은 비즈니스 관점에서 전사적인 위험관리 수행이 필요하다고 할 수가 있다[3].

조직이 직면한 위험을 식별 및 평가하고 완화 하도록

하는 위험관리 표준인 ISO31000:2018 에서는 변화하는 비즈니스 및 시장의 상황과 조직이 직면한 새로운 위험을 고려하고, 지속적으로 변화하는 사회에서의 불확실성이 증가함에 따라 개정작업이 이루어졌다. 개정된 내용을 살펴보면 비즈니스 가치창출과 자산보호라는 목표를 설정하였으며, 위험관리를 조직의 비즈니스 목표와 상황에 맞게 정의, 이해관계자의 적절한 참여, 최고경영진의 의사결정에 대한 책임을 강조하였다[8].

COSO ERM(2017)은 위험관리가 전략 수립과 조직 활동 전반에 적용되며, 위험 불확실성에 직면한 경영진이 효율·효과적으로 위험을 인식 및 평가, 관리할 수 있도록 도와주는 전사적 위험관리 모델로서 2017년 개정이 이루어졌다. 개정작업이 이루어진 이유는 컨설팅 그룹인 프라이스워터하우스(PwC) 조사 결과, 실적이 저조한 기업의 80%가 전략적 실수로 인해 실패를 경험하였으며, 비즈니스 목표를 달성하기 위해서는 일정수준의 위험을 감수 하는 게 필요하고 조직의 핵심가치와 위험에 대한 태도를 직원의 행동과 일치시킬 필요가 있다고 보았기 때문이다[4].

이처럼 앞서 개정된 두 위험관리 모델을 분석한 내용을 종합해보면, 변화하는 비즈니스 환경에 대응하고 비즈니스 목표를 달성하기 위해 개정작업이 이루어졌다고 할 수가 있다. 특히 COSO ERM모델에서는 전사적 측면에서 기업의 목적을 달성하기 위한 합리적 대응 방안을 모색하고, 기업의 목표 달성에 영향을 주는 잠재적인 위험을 파악하여 일정한 수준 내에서 위험을 적절히 관리해야하며, 조직이 목표를 추구할 때 위험성향의 중요성을 강조하고 있다고 할 수가 있다[4,8].

또한 정보보안 위험관리 프레임워크인 ISO/IEC 27005에서는 상황설정단계에서 조직에 영향을 미치는 위험관리의 목적을 결정하고, 법규 및 규정 측면, 운영, 기술, 재무, 사회 및 인적요인을 고려하여 위험수용 기준을 설정해야한다고 명시하고 있다. 이는 보안 위험관리의 전략을 세우는 중요한 활동으로서, 허용이 가능한 위험의 수준(Acceptable Level of Security Risk)을 결정하는 것이며, 위험처리 시 발생하는 위험회피, 위험전가, 위험감소, 위험수용 등 의사결정에서의 판단 기준을 제공한다고 할 수가 있다[9].

2.2 위험성향(Risk Appetite)의 개념

2.2.1 전통적 위험성향

위험성향은 불확실성하에서 사람의 의사결정을 설명하기 위해, 고안되어진 개념이라고 할 수가 있다[10]. 위험성향은 새롭게 대두된 개념이 아니며 개인의 투자와 관련하여 재무 분야에서 위험성향이라는 개념이 오랫동안 사용되어져 왔다.

마취와 사피라(1987)는 부정적인 결과가 발생하더라도 인간이 선택하게 되는 부정적인 결과의 정도로 투자결정에 영향을 주는 변수라고 하였으며, 어윈(1993)은 인간의 행동의 결과가 불확실하거나 손실의 확률이 있을 때 행동에 기꺼이 참여하려고 하는 정도로 정의하였다[11,12]. 경제학적으로 위험에 대한 성향은 주관적인 성향으로 인간의 심리적, 사회·경제적 특성 및 상황에 따라 다르다고 알려져 있다[10].

인간의 위험성향을 조직의 관점으로 생각해보면, 위험성향은 조직이 비즈니스 목표달성을 위해서 기꺼이 감당할 수 있다고 생각하는 위험의 크기라고 할 수가 있다. 조직의 위험성향은 절대적인 개념이 아니고 위험추구와 위험회피의 연속체 상에 위치하는 개념이지만 조직이 수용할 수 있는 손실의 정도에 따라 위험 회피형, 위험 중립형, 위험 추구형으로 구분되어진다[13].

2.2.2 보안 위험성향

글로벌 컨설팅 그룹인 가트너(Gartner)에서는 성공한 기업들과 실패한 기업들을 구분하는 것은 올바른 위험을 감수할 수 있는 능력이며, 각 기업의 위험성향에 맞는 위험을 구분하고 관리하는 능력들이 중요한 것으로 보았다. 또한 Fig. 1에 제시되어 있는 것처럼 위험을 High Risk 대 Low Risk에서, Good Risk 대 Bad Risk의 관점으로 보아야함을 강조했다. 즉 위험관리를 단순히 위험의 가능성과 영향에 관점에서 고위험을 줄이거나 회피함으로써 손실을 최소화하거나 제거하는 것에서 벗어나, 위험을 수용했을 때의 창출되는 가치와 위험부담을 충분히 평가할 때 좋은 위험이 될 수 있는 것을 본 것이다[14].

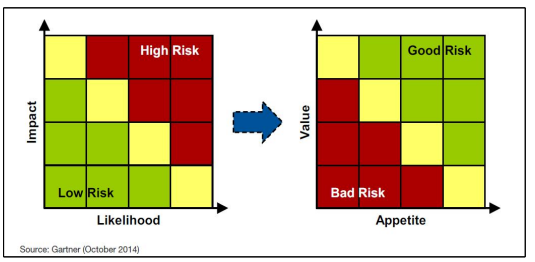

Fig. 1. Shifting the Risk Conversation

앞서 언급한 ISO 31000위험관리 프레임워크와 COSO ERM에서는 위험성향을 조직이 추구하거나 보유할 준비가 된 위험의 양과 유형, 조직이 가치를 추구하여 기꺼이 수용할 위험의 양으로 위험성향의 정의를 내리고 있다[4,8].

글로벌 컨설팅 그룹인 프라이스워터하우스쿠퍼스(PwC)에서는 위험성향을 조직의 전반적인 위험수용 가능범위 내에서 회사가 수용하고자 하는 위험의 양이라고 정의를 내리며, 위험성향과 문화 간의 관계, 경제적 자본에 있어서 위험성향을 고려해야한다고 언급하였다[15]. 딜로이트(Deloitte)와 정보 시스템 감사·조정협회(ISACA)에서도 조직이 목표를 달성하기 위해 기꺼이 받아들이는 위험의 양으로 정의를 하며, 위험회피 및 위험전가 비용을 고려하고 위험성향을 표현하기 위해 등급화된 척도를 마련할 필요가 있으며, 위험을 재무뿐만 아니라, 비재무적인 요소도 고려하는 등 단일적으로 보는 관점이 아닌 전사적으로 보아야한다고 강조하였다[16,17]. 조직 전사적인 관점의 위험성향에 대한 정의를 정리하면 다음 Table 1과 같다.

Table 1. Definition of Risk Appetite

Source	Definition of Risk Appetite
ISO[8]	Amount and type of risk that an organization is prepared to pursue or retain
COSO[4]	The amount of risk an entity is willing to accept in pursuit of value
PwC[15]	The quantum of risk that the firm is willing to accept within its overall capacity
Deloitte[16]	The risk a firm is willing to take in the pursuit of its strategy.
ISACA[17]	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission

2.3 보안 위험관리 의사결정

2.3.1 보호동기 이론(Protection Motivation Theory)

보호동기 이론은 건강과 관련한 태도 및 행동을 설명하기 위하여 Rogers RW(1975)가 개발한 이론이라고 할 수가 있으며, 건강 및 안전과 관련되어진 위협적인 메시지에 노출되었을 경우, 보호동기를 유발시켜 자신을 보호하려는 행동의 변화를 불러일으킨다는 가정을 기반으로 메시지의 효과를 설명하기 위해 개발되어진 이론이라고 할 수가 있다[18,19].

보호동기 요인은 위협평가와 대응평가로 구분되며, 다시 위협평가는 인지된 심각성(Severity), 인지된 취약성(Vulnerability)으로, 대응평가는 자기 효능감(Self efficacy), 반응 효능감(Response Efficacy)으로 구분할 수가 있다[18,19].

보건학, 교육학 심리학 등 다양한 분야에서 보호 행동을 설명하기 위하여 사용되어진 보호동기이론은 조직의 보안 위험관리와도 관계되어진다. 이러한 보호동기 이론을 바탕으로 안효주 외 2명(2015)은 인지된 심각성, 인지된 취약성, 반응 효능감, 자기효능감 등을 보안 위험관리 의사결정에 영향을 미치는 요소로 보았다. 인지된 심각성을 조직 구성원의 부주의로 발생할 수 있는 보안 침해사고의 심각성에 대한 인식으로 설명하며, 인지된 취약성을 위험을 관리하지 않을 시 정보자산이 취약해질 수 있는 가능성으로 보았다. 또한 자기효능감은 보안 위험을 관리하기 위한 기술, 지식 및 능력에 대한 확신의 정도로, 반응 효능감을 보안 위험을 줄이기 위하여 사용되는 보안 대책의 효과성으로 보았다[20].

2.3.2 기타 보안위험관리 의사결정에 관한 연구

보안 위험관리의 중요성과 필요성에 비해서는 보안위험관리 의사결정에 미치는 요인과 관련된 연구가 아직 많이 부족한 실정이며, 다양한 관점에서의 연구가 미미한 실정이다. 송영미·김상현(2012)은 조직의 보안위험관리 의사결정에 영향을 미치는 인지요인으로 보안 관리행동, 보안의무의 준수, 인식된 이득, 사회의 압력, 보안위험의 경험을 강조하였다[21]. 보안 관리행동의 경우, 조직 구성원의 보안 위험 관련 행동 또는 보안 실천의 정도, 보안의무의 준수는 조직의 보안 정책 또는 지침을 준수하고 따르는 정도, 지각된 이득은 보안 위험관리를 통하여 얻게 되는 유형 및 무형의 이득에 대한 인식의 정도로 보았다. 또 사회적 압력의 경우는 동종 산업 보안 위험관리에 대한 의사결정 또는 인식의 정도, 보안위험의 경험을 보안위험의 직·간접적 노출 및 경험의 정도로 인식하였다.

2.4 시사점

보안에 대한 위험은 디지털 기술의 발달로 인해 점점 다양해지고 고도화되고 있다. 이에 위험관리에 대한 중요성이 나날이 커지고 있으며, 보안 위험관리에 대한 접근법도 변화될 필요성이 있다. 보안 위험관리는 부분적으로 수행하는 활동이 아닌, 비즈니스 중심의 전사적으

로 수행되어야하며, 비즈니스 목표를 달성하기 위해 보안 위험을 기꺼이 수용할 수 있는 위험의 크기를 뜻하는 보안 위험성향 파악에 대한 중요성이 대두되고 있다.

위험성향은 전통적으로 개인의 투자 의사결정과 관련하여 연구가 많이 진행되어져 왔으며, 기존 위험관리 프레임워크의 보안 위험성향 측정 및 조직의 보안 위험성향 관련 연구도 미미한 실정이다. 이에 ISO/IEC 27005에서 제시하고 있는 위험수용 고려 기준과 전사적 위험성향 프레임워크에서 제시하고 있는 재무 및 비재무적 고려사항, 보안 위험관리 의사결정에 영향을 미치는 요인을 분석하여 조직의 보안 위험성향을 파악할 수 있는 프레임워크를 개발할 필요가 있다.

3. 보안 위험성향 프레임워크의 개발 및 검토

3.1 보안 위험성향 프레임워크 개발

위험성향 측정에 대한 구체적인 연구가 미흡하고 부족한 실정이기 때문에, 앞서 이론적 배경 및 선행연구를 통해 제시한 ISO/IEC 27005의 위험수용 고려 기준을 기반으로 하여, ISACA, PwC, Deloitte, The British Library 위험성향 프레임워크 관련 연구에서 제시하고 있는 위험성향 고려분야를 매핑 하여, 보안 위험성향 측정 시 필요한 재무, 운영, 기술, 문화, 평판, 컴플라이언스 6가지 위험분야를 도출하였다. 또한 보호동기이론, 기타 보안 위험관리 의사결정에 영향을 미치는 요인을 분석 및 매핑 하여, 각 위험분야 마다 측정해야하는 인지된 심각성(Severity), 인지된 취약성(Vulnerability), 자기 효능감(Self Efficacy), 반응 효능감(Response Efficacy)의 4가지 요인을 도출하였다. 도출한 주요 분야 및 요인은 다음 Table 2와 같다.

Table 2. Key Domain & Factor of Security Risk Appetite

Risk Domain	Reference	Decision Factor	Reference
Financial	ISO/IEC27005(2014), ISACA(2013), PwC(2016), Deloitte(2014), British Library(2017)	Severity	Rogers RW(1975), Hoju An, et el.(2015)
Reputation	PwC(2016), Deloitte(2014), British Library(2017)	Vulnerability	Rogers RW(1975), Hoju An, et el.(2015)
Compliance	ISO/IEC27005(2014),PwC(2016), Deloitte(2014), British Library(2017)		
Culture	ISO/IEC 27005(2014), PwC(2016), Deloitte(2014), British Library(2017)	Response Efficacy	Rogers RW(1975), Hoju An, et el.(2015)
Operation	ISACA(2013), ISO/IEC27005(2014), Deloitte(2014), PwC(2016), British Library(2017)	Self-Efficacy	Rogers RW(1975), Hoju An, et el.(2015)
Technology	ISO/IEC27005(2014), ISACA(2013), Deloitte(2014), British Library(2017)		

Fig. 2에 표현되어 있는 것처럼, 기업의 달성하고자하는 보안의 목표의 수준에 따라 비즈니스 보호 중심, IT자산 보호 중심으로 구분되어질 수 있으며, 보안 위험성향 측정 시 고려해야할 위험분야로 재무, 평판, 컴플라이언스, 문화, 운영, 기술 분야가 구성된다. 재무위험은 조직에서 보안사고 발생 시 재정적 손실 및 경제적 비용을 이야기 하며, 평판위험은 보안사고 발생 시 대중들이 인식하고 있는 기업 및 브랜드 평판가치의 하락을 말한다. 컴플라이언스 위험은 법규 및 규제사항 미 준수에 따른 감독 당국의 압력 및 계약 위반사항을, 문화위험은 미흡한 경영진 및 직원들의 보안 인식 및 회피습관을 말한다고 할 수가 있다. 또한 운영위험은 정보시스템 운영에서의 오류 및 장애로 인한 업무중단, 기술위험은 미흡한 암호화, 접근통제 등에 따른 위험으로 정의할 수가 있으며, 각 위험분야마다 위협평가, 대응평가로 나뉘어지는 인지된 심각성(보안 침해사고에 대한 심각성에 대한 인식), 인지된 취약성(정보자산이 취약 해질 수 있는 가능성), 반응 효능감(보안 대책에 대한 효과성), 자기 효능감(보안 위험관리에 대한 지식 및 능력의 확신)을 측정할 수가 있다.

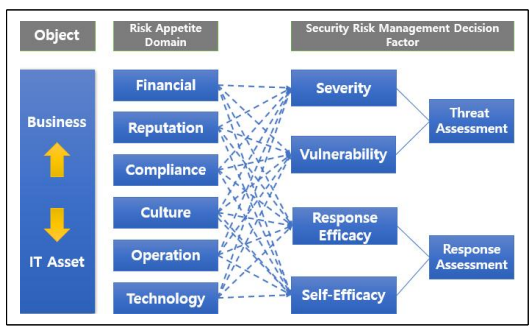

Fig. 2. Framework for Measuring Security Risk Appetite

3.2 전문가 검토 및 결과

본 연구는 위험관리 및 위험성향 프레임워크, 위험성향 선행연구를 분석하여, 6개의 보안 위험성향 고려분야와 4개의 측정요인을 개발하였다. 6개의 보안 위험성향 고려 분야는 ISO/IEC 27005의 위험수용 고려 기준을 기반으로 도출하였으며, 4개의 측정요인은 보호동기이론의 가장 기본 요인이라고 할 수 있는 요인을 기반으로하여 측정요인을 도출하였다. 보안 위험성향 및 위험관리에 대한 국내 연구 현황을 고려하였을 때, 정량적인 방법으로는 심도 있는 결과를 도출하기 어렵다고 판단하였다. 따라서 개발되어진 프레임워크에 대해 중요성과 실현가능성을 검토하는 포커스 그룹 인터뷰(FGI) 방법을 사용하였다. 포커스 그룹은 주제와 관련하여 공통된 특성을 가진 전문가들 간의 상호작용을 통해서, 연구주제에 관하여 자료를 수집하는 방식이다[22]. Table 3과 같이 위험관리 관련 프로젝트 경험이 있는 컨설턴트, 보안 위험관리 전문가들로 구성했으며, 참여자는 모두 10년 이상의 경력을 보유했다.

Table 3. Focus Group Interview Members

	Group Members	Member's Speciality
1	Consultant 1	Risk Management
2	Consultant 2	Risk Management
3	Security manager 1	Security Management
4	Security manager 2	Security Management
5	Senior Researcher 1	Governance, Risk and Compliance
6	Senior Researcher 2	Governance, Risk and Compliance

본 연구에서 수행된 포커스 그룹 인터뷰(FGI) 절차는 다음과 같다. 1차 검토에서는 위험관리 프레임워크 선행연구 분석을 기반으로 위험 수용 고려 분야에 대해 의견수렴 절차를 진행하고, 2차 검토에서는 각 위험분야에 대한 측정요인 검토를 진행하였다. 마지막 3차 검토에서는 개발되어진 프레임워크에 대하여 설문지 작성 및 심층면접을 수행하였다. 설문지는 개발된 프레임워크의 중요성과 실현가능성을 리커드 5점 척도를 사용해, 조사했으며, 추가로 개선사항 또는 제언에 대해 작성하도록 하였다. 또한 설문 후에는 약 60분에 걸쳐 토론 및 의견교환의 시간을 진행하여 프레임워크의 타당성을 검토했다.

보안 위험성향 측정 프레임워크의 기각 및 채택 기준은 카프레라(Cabrera)의 연구를 참고하여 실현가능성과 중요성 모두 2.5 이상인 경우는 채택, 하나의 항목만 2.5 이하인 경우에는 기각 및 채택의 여부를 전문가 검토 및 의견 수렴 후에 결정하였다[23]. 반면에 중요성과 실현가능성이 모두 2.5 이하인 경우는 기각하였다.

Table 4와 같이 검토결과, 6개의 각 위험 분야별 4개의 측정요인들의 중요성과 실현가능성 모두 2.5이상으로 높게 검토되어, 보안 위험성향 측정 지표로서 타당한 것으로 채택되었다. 그러나 위험분야와 측정항목중 상대적으로 낮은 3.0이하가 1개 검토되었는데, 그 이유는 다음과 같다.

위험수용고려분야 중 운영위험의 경우, 다른 위험분야와의 경계가 모호하며, 특히 기술위험에 포함되어져 있는 내·외부 위협에 관한 사항은 운영위험과 깊은 관련성이 있기 때문에 중복된다는 의견이 다수였다. 그렇기 때문에 운영위험과 기술위험을 구분 짓기 위해서는 측정지표 도출시, 명확하게 정의를 내릴 필요가 있을 것으로 검토되었다.

또한 기타의견으로 보안사고 경험이 나왔으나, 보안사고 경험은 2017년 정보보호실태조사의 통계자료를 예로 들면서, 침해사고를 경험한 응답자의 54.6%는 사용 중인 비밀번호 변경, 보안 소프트웨어 설치, 개인정보 공개중단, 서비스 공급업체 변경 등 구체적인 대응활동을 수행하고 있지 않으며, 침해사고 경험 이후에 기관이나 업체에 상담이나 문의를 받지 않은 경우는 52.6%로 보안사고의 경험이 위험성향을 파악할 수 있는 중요한 근거가 될 수 있는지는 추가적 연구가 필요해 보인다는 검토결과가 있었다.

추가로 위험성향 파악을 위해서는 위험성향 측정 프레임워크도 중요하지만 더 나아가 각 위험분야 및 측정요인에 대한 지표들이 개발될 필요성이 강조되었으며, 측정된 위험성향을 가시적으로 분류하고 전략을 세울 수 있는 위험성향의 활용방안도 개발될 필요가 있다고 검토되었다.

Table 4. Review of Framework for Measuring of Security Risk Appetite using FGI

Risk Domain	Decision Factor	Materiality	Feasibility
Financial	Severity	3.8	3.5
	Vulnerability	3.8	3.5
	Response Efficacy	3.5	3.3
	Self-Efficacy	3.2	3.0
	Average	3.6	3.3

Reputation	Severity	3.8	3.3
	Vulnerability	3.8	3.3
	Response Efficacy	3.7	2.8
	Self-Efficacy	3.5	3.2
	Average	3.7	3.2
Compliance	Severity	3.0	3.5
	Vulnerability	3.3	3.2
	Response Efficacy	3.2	3.2
	Self-Efficacy	3.3	3.2
	Average	3.2	3.3
Culture	Severity	4.2	3.2
	Vulnerability	3.5	3.2
	Response Efficacy	3.5	3.3
	Self-Efficacy	3.8	2.8
	Average	3.8	3.1
Operation	Severity	3.5	2.6
	Vulnerability	3.0	2.8
	Response Efficacy	3.3	2.8
	Self-Efficacy	3.7	2.8
	Average	3.4	2.8
Technology	Severity	4.2	3.7
	Vulnerability	3.7	3.2
	Response Efficacy	4.0	3.2
	Self-Efficacy	3.8	3.3
	Average	3.9	3.4
Factor Aggregate	Severity	3.8	3.3
	Vulnerability	3.5	3.2
	Response Efficacy	3.5	3.1
	Self-Efficacy	3.6	3.1
	Average	3.6	3.2

4. 결론

본 연구는 비즈니스 목표 달성을 위한 위험관리 방안의 초기 활동 및 미비한 위험 수용 수준 측정 기준에 있어서의 보완점을 제시해줄 수 있는 위험성향 측정 프레임워크를 개발하였다. 기존 위험성향에 대한 연구는 개인의 투자 위험 성향에 대한 연구로서 논의가 이루어졌었으며, 조직의 전사적인 관점에서의 위험성향에 대한 연구는 포괄적으로 방향성을 제시해줄 뿐 측정요인에 대한 구체적인 연구가 부족한 실정이며, 보안위험 특성에 적합한 고려요소를 제시하지 못했다. 그렇기 때문에 개발된 보안 위험성향 프레임워크는 조직이 실무적으로 위험성향을 파악하는데 있어 참고모델이 될 수 있으며, 변화하는 위험 패러다임에 따른 비즈니스 중심의 위험관리 접근에 중요한 의미를 지닐 것으로 사료되어진다.

본 연구의 한계점은 보안 위험성향에 관한 연구가 미미한 실정에 따라 포커스 그룹 인터뷰로 중요성과 실현가능성을 검토하였기 때문에 일반화에 대한 어려움이 존재한다. 따라서 향후 요인분석, 다변량 분석 등 정량적인 연구가 필요할 것으로 보이며, 향후 위험성향 프레임워크를 활용하여 측정지표를 개발하고, 위험성향의 유형을 가시적으로 분류할 수 있는 활용방안에 대한 연구가 필요할 것으로 보인다.

보안 위험성향은 조직의 상황을 고려한 위험관리 전략의 하나로써, 보안 관리 활동의 근본이지만 아직 제대로 수행되지 못한 위험관리 활동의 첫 발 내딛음을 하는 중요한 역할을 수행할 것으로 기대한다.

REFERENCES

[1] J. D. Kim & C. G. Jin. (2016). International Standardization Trends and Issues of Cyber Resilience, *Review of KIISC, 26(4),* 11-15.

[2] *Cybersecurity as a Growth Advantage.* (2016). San Jose:CISCO.

[3] *A new posture for cybersecurity in a networked world.* (2018). New York:Mckinsey.

[4] COSO ERM Integrating with Strategy and Performance. (2017). California:COSO.

[5] G. Stoneburner, A. Goguen & A. Feringa. (2002). *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology.* Gaithersburg:NIST.

[6] M. E. Whitman. (2003). Enemy at The Gate: Threats to Information Security. *Communications of the ACM, 46(8),* 91-95.

[7] *Achieving Resilience in the cyber ecosystem.* (2014). London:Ernst & Young.

[8] *Risk management 31000.* (2018). ISO, Switzerland, ISBN 978-92-67-10784-4.

[9] ISO/IEC. *ISO/IEC 27005:2014.* (2014). Geneva:ISO.

[10] W. S. Kim & J. H. Min. (2018). A Practical Approach to Measuring the Risk Attitudes of Individual Investors. *Journal of the Korean Operations Research and Management Science Society, 43(1),* 1-19.

[11] J. G. March & Z. Shpira. (1987). Managerial Perspectives on risk and risk taking. *Management Science, 33(11),* 1404-1418.

[12] C. E. Irwin Jr. (1993). *Adolescence and risk taking: How are they related.* Thousand Oaks:SAGE Publications.

[13] S. H. Joung & M. K. Shin. (2011). A Study on the Related Variables to Financial Risk Tolerance and the Ratio of Risky Asset Possession. *Financial Planning Review, 4(4),* 1-20.

[14] The Gartner Strategic Risk Evaluation Approach for Digital Business. (2014). Stamford:Gatner.

[15] B. Richard. (2016). *Risk appetite - How hungry are you?.* London:PwC.

[16] *Risk appetite frameworks How to spot the genuine article.* (2014). New York:Deloitte.

[17] P. Mukul. (2013). *What Is Your Risk Appetite?.* Illinois:ISACA.

[18] S. H. Jang & E. J. Yoon. (2016). A Comparative Study on the Awareness of Health Risks and the Risk Reduction Measures Related to Sodium Intake between Female and Male University Students in Busan and Gyeongnam : An Application of Protection Motivation Theory. *Korean Journal of Food and Cookery Science, 32(1),* 136-146.

[19] R. W. Rogers. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook,* 153-176.

[20] H. J. An, J. Y. Jang & B. S. Kim. (2015). Factors Drawing Members of a Financial Institution to Information Security Risk Management. *Information Systems Review, 17(3),* 39-64.

[21] Y. M. Song & S. H. Kim. (2012). A Study on the Impact of the Security Risk Management Awareness Management in the Organization. *Korean Association Of Industrial Business Administrarion,* 425-440.

[22] David L. Morgan. (2007). *Foucs groups as qualitative research.* Seoul:KOONJA.

[23] D. Cabrera, J. T. Mandel & J. P. Andras. (2008). What is the crisis? efining and prioritizing the world's most pressing problems. *Front Ecol Environ, 6(9),* 469-475.

김 기 삼(Gim, Gisam) [학생회원]

- 2015년 2월 : 상지대학교 경영정보학과(학사)
- 2017년 3월 ~ 현재 : 중앙대학교 산업융합보안학과(석사과정)
- 관심분야 : 보안 위험관리, 디지털 비즈니스 보안, 보안 거버넌스
- E-Mail : clear1117333@gmail.co.kr

박 진 상(Park, Jinsang) [학생회원]

- 2017년 8월 : 중앙대학교 경영학과(학사)
- 2017년 9월 ~ 현재 : 중앙대학교 융합보안학과(석사과정)
- 관심분야 : 보안 거버넌스, 블록체인, 이상징후 감지시스템
- E-Mail : pongoboy516@gmail.co.kr

김 정 덕(Kim, Jungduk) [종신회원]

- 1979년 2월 : 연세대학교 정치외교학과(학사)
- 1981년 8월 : 연세대학교 경제학과 대학원(석사)
- 1986년 8월 : Univ. of S. Carolina, MBA
- 1990년 12월 : Texas A&M Univ., Ph. D. in MIS
- 1995년 3월 ~ 현재 : 중앙대학교 산업보안학과 교수
- 관심분야 : 디지털 비즈니스 보안, 산업보안 거버넌스 및, 보안관리
- E-Mail : jdkimsac@cau.ac.kr