J. Soc. Korea Ind. Syst. Eng Vol. 39, No. 3 : 18-29, September 2016
http://dx.doi.org/10.11627/jkise.2016.39.3.018
ISSN : 2005-0461(print)
ISSN : 2287-7975(online)

Study on Development of Framework of Company Classification in Information Security Perspective

Hee-Ohl Kim* · Dong-Hyun Baek**†

*Graduate School of Management Consulting, Hanyang University
**Department of Business Administration, Hanyang University

정보보호 관점의 기업 유형 분류 프레임워크 개발에 관한 연구

김희올* · 백동현**†

*한양대학교 일반대학원 경영컨설팅학과
**한양대학교 경상대학 경영학부

For most organizations, a security infrastructure to protect company's core information and their technology is becoming increasingly important. So various approaches to information security have been made but many security accidents are still taking place. In fact, for many Korean companies, information security is perceived as an expense, not an asset. In order to change this perception, it is very important to recognize the need for information security and to find a rational approach for information security. The purpose of this study is to present a framework for information security strategies of companies. The framework classifies companies into eight types so company can receive help in making decisions for the development of information security strategy depending on the type of company it belongs to. To develope measures to classify the types of companies, 12 information security professionals have done brainstorming, and based on previous studies, among the factors that have been demonstrated to be able to influence the information security of the enterprise, three factors have been selected. Delphi method was applied to 29 security experts in order to determine sub items for each factor, and then final items for evaluation was determined by verifying the content validity and reliability of the components through the SPSS analysis. Then, this study identified characteristics of each type of eight companies from a security perspective by utilizing the developed sub items, and summarized what kind of actual security accidents happened in the past.

Keywords : Information Security, Evaluation Index, Development of Framework, Company Classification

1. 서 론

대부분의 조직에서 핵심 자산으로 분류되는 정보와 기술을 보호하기 위한 보안 환경 구축과 이에 대한 운영 업무는 그 어떤 업무보다 중요해지고 있다. 이에 따라 다양한 방법으로 정보보안에 대한 접근이 이루어지고 있지만, 보안 사고는 지속적으로 발생하고 있으며 그 빈도나 피해 규모 역시 줄어들지 않고 있다[25]. 기업의 중요한 정보를 위협하는 기술이나 방법들이 하루가 다르게 지능화 되고 있는 것에 반해 대기업 등 일부 기업을 제외하면 대부분 내부적으로 정보보호 정책조차 수립되어 있지 않은 기업이 대부분이며, 자체적으로 보안 역량을 쌓기보다는 단순히 외부의 보안업체 혹은 보안 솔루션 제공 업체에 의존하고 있는 현실이다[11]. 또한 정보보안 관련

Received 19 July 2016; Finally Revised 29 July 2016;
Accepted 30 July 2016
† Corresponding Author : estarbaek@hanyang.ac.kr

분야는 투자 대비 수익률(ROI) 산출이 쉽지 않고 설령 측정 된다 해도 공격의 인지 및 해당 공격에 대한 직접적인 피해가 발생했을 경우 사후 측정이 대부분이기 때문에 경영진 입장에서 적절한 보안 투자를 결정하는데 있어서 선택을 망설이게 하는 요소로 작용한다[6, 25]. 나날이 발전하고 있는 해킹, 바이러스와 같은 기술적 위협을 완벽하게 방어하는 것은 사실상 불가능에 가까우며, 이에 소모되는 비용 또한 우리나라의 기업 정서상 지속가능한 성장과 안정성에 대한 미래의 투자 개념이 아닌 소모성이 짙은 매몰 비용으로 인식하고 있다[1, 7, 8, 12, 16, 21, 27, 28]. 이러한 매몰 비용 혹은 함몰 비용이라는 기본적인 인식을 바꾸려면 기업이 왜 보안에 투자를 해야 하고, 누가 집행할 것이며, 어느 곳에 어느 정도의 투자를 해야 그에 따른 효과를 극대화 할 수 있는지 등에 대한 분석이 필요한데 이에 대한 연구는 거의 진행되지 않았을 뿐더러 개별 기업의 특성을 고려하지 않은 것들이 대부분이다[5, 8, 14, 15, 32, 37, 38].

현재 정보보안을 도입하고 있는 기업들 대부분은 한국 인터넷 진흥원에서 인증하고 있는 정보보호 관리 체계(ISMS) 가이드라인 기반의 통제 항목을 바탕으로 보안 업무를 수행하고 있다. 그리고 제조업과 같은 첨단 기술에 대한 보안이 필요한 분야의 경우 부정경쟁방지 및 영업비밀보호에 관한 법률 및 산업기술보호의 유출방지 및 보호에 관한 법률에 의거하여 특허제도와 영업비밀 보호제도를 이용하여 산업기술에 대한 보호를 받는다. 하지만 위의 제도들은 규모가 작은 중소기업들의 경우 제대로 된 혜택을 누리기가 힘든 것이 현실이다. 기업 규모가 커서 인력과 예산을 투입하는데 비교적 수월한 대기업과 달리 열악한 환경의 중소기업은 정보보호에 대한 지식과 경험이 부족할 뿐만 아니라 자체적인 전담 조직을 꾸리는 데에도 어려움을 겪고 있어 기업 상황에 맞는 전략 수립이 거의 불가능하기 때문이다[5, 8, 14, 32].

앞서 언급했듯이 정보보안에 접근하고자 하는 기업들은 보안 솔루션이나 방화벽, 네트워크 보안과 같은 기술적인 이슈에만 단순하게 집중하는 경향이 있다[4, 7, 19, 32, 37]. 이는 정보보안을 연구하는 학계에서도 마찬가지인데, 대부분의 연구나 정책들이 기술적인 관점에서 각각의 솔루션들의 보안성과를 평가하거나 ISMS와 같은 평가 체계로 기업의 보안 역량에 대해 분류하는 연구를 진행해왔다. 하지만 정보보안에 접근할 때 모든 기업이 일관적이고 단편적인 접근 방법을 사용하는 것은 이미 많은 보안사고 사례를 통해 알 수 있듯이 효율적인 방법이 아니다. 이는 정보보안 자체의 성격이 복합적이고 다면적이며 동적인 특징을 가지고 있기 때문이기도 하며, 개별 기업이 가지고 있는 성격이나 당면해 있는 환경 또는 상황 또한 매우 많은 다양성을 지니고 있기 때문이다[16, 19, 26, 28].

정보보호에 대한 효과적인 접근을 위해서는 기업이 처한 상황이나 환경, 보호해야 할 정보의 형태, ICT 인프라 등 전반적인 내용들이 함께 고려되어져야만 한다. 본 연구의 목적은 정보보안에 접근하고자 하는 기업의 상황에 맞는 전략 유형 프레임워크를 제시하는데 있다. 이 프레임워크는 기업의 유형을 8가지로 분류하는데, 각 기업은 자사가 속한 유형에 따라 정보보안 전략 수립 의사결정을 지원 받을 수 있다. 본 연구에서는 기업의 유형을 분류하기 위한 프레임워크 개발을 위해 보안 관련 전문가 12명과 브레인스토밍을 진행하고 선행 연구를 바탕으로 기업의 정보보안에 영향을 미칠 수 있다고 검증된 요인 가운데 양극의 영향 요인 3가지를 선정하였다. 그리고 각각의 요인 별로 세부 척도 항목을 다시 29명의 보안 관련 전문가를 대상으로 델파이(Delphi) 기법을 활용하여 개발한 후 SPSS 분석을 통해 구성 요인의 내용타당도 및 신뢰도를 검증하여 최종 평가 항목을 도출하였다. 기업은 하나의 역동적인 유기체이며, 외부환경과 끊임없이 상호작용하는 사회적 체계이다. 사람들 개인이 서로 다른 체형이나 성격을 지니고 있듯이 기업들도 규모나 구조가 다르며 수행하는 업무의 목적에 따라 다양한 분류가 가능하다. 본 연구는 정보보안의 효과적인 구현을 위한 성공 요인으로 기업이 근본적으로 가지고 있는 성격에 대한 분석이라고 보고 분석에 사용될 프레임워크를 개발하는 연구를 진행하였다. 그리고 개발된 프레임워크를 활용하여 보안의 관점으로 본 8가지 기업의 유형은 각각 어떤 특징을 가지고 있으며, 주로 해당되는 기업과 실제 사고 사례에 대해 정리해 보았다. 본 연구의 결과는 처음 정보보안에 접근하고자 하는 기업이나 새롭게 정보보안 전략을 수립하고자 하는 기업에 기초가 될 자료로서 의사결정을 지원할 결과를 산출하는데 도움을 줄 것으로 기대한다.

2. 선행 연구와 이론적 배경

2.1 정보보안에서 조직과 기업 유형 분류의 필요성

사람들이 서로 다른 체형과 성격을 지니고 있듯이 조직이나 기업들도 규모나 구조 등이 서로 다르며 지향하는 목적에도 차이가 있다. 즉, 기업 간에 다른 기업과는 구별되는 고유한 특성이 존재한다는 이야기이다. 예를 들어, 어떤 기업은 상대적으로 외부 지향적인 반면에 어떤 기업은 상대적으로 내부 지향적일 수 있고, 방어적인 전략을 사용하는 기업이 있다면 반대로 공격적인 전략을 선호하는 기업이 있을 수 있다. 실제로 한 산업 내의 기

업들은 그들이 활용하는 유통채널, 세분시장, 제품의 질, 기술력, 소비자에 대한 서비스, 가격, 마케팅 전략 등의 측면에서 서로 다른 전략을 구사한다[10, 29]. 조직은 하나의 역동적인 유기체이며 외부환경과 끊임없이 상호작용하는 사회적 체계이다[16, 17, 26]. 기업의 특성은 기업이 추구하는 목적이나 수행하는 기능, 처한 상황이나 환경, 경영진의 성향 등에 영향을 받아 형성된다[26, 30]. Phares[29]는 개인의 성격을 “시간과 환경에 따라 형성되며 한 개인을 다른 사람과 구별해 주는 특징적인 사고, 감정 및 행동양식”이라고 정의하였는데 이러한 정의를 기업의 성격으로 대입해 보면 “시간과 환경에 따라 형성되며 한 기업을 다른 기업과 구별해 주는 특징적인 속성, 기질 및 행동양식”이라고 정의해볼 수 있다. 조직과 기업을 연구하는 학자들은 기업의 궁극적인 목표가 성과의 실현에 있기 때문에 시장 지배를 위해서 개별 기업이 맞춤형 전략을 사용할 필요가 있다는 연구를 진행해왔다. 하지만 많은 연구에서 기업이 대체로 유사한 것처럼 생각하고 연구를 수행하고 있다[23]. 심지어 적은 표본을 기초로 한 연구결과를 모든 기업에 일반화 시키는 경향도 있으며, 표본이 갖는 대표성에 관하여 보다 심도 있는 토의도 없이 그 결과의 일반화 가능성을 보증한다는 가정을 가지고 단순하게 일반화시키기도 해왔다[30]. 조직의 형태(organizational configuration)는 조직의 전략, 구조, 과정들의 속성들이 공통적으로 나타나는 군집들(clusters)로 정의할 수 있다[24, 25]. 정보보안에 접근하는데 있어서도 기업들을 일관적인 기준을 가지고 접근하는 방법보다 기업들이 가지고 있는 특성, 내적 일관성 등을 구분해 봄으로써 기업 현상을 보다 잘 이해할 수 있는 접근 방법을 택하는 것이 보안 전략을 세우는데 유리할 것이다. Sanchez[31]는 일정한 기준에 따라 분석대상을 분류함으로써 효율성과 예측의 가능성을 높여준다고 하였고, Rich[25]은 기업을 분류하여 집단적인 범주나 군집으로 나누는 것은 기업의 연속적인 상태를 파악하기에 적합한 방법이라고 하였다.

2.2 주요 정보보호 관리체계 프레임워크 구성과 문제점

서론에서 밝혔던 것과 같이 정보보안을 도입하고 있는 기업들은 정보보호 관리체계 프레임워크를 활용하여 보안 전략을 세워놓고 있다. 하지만 접근 방법이 현재 기업의 보안 상태를 점검하기 위한 수준 진단에 그칠뿐더러 인증을 획득하기 위한 수단에 불과하여 실제 정보보안의 효과로 이어지는 것과는 거리가 있다는 것이 여러 사고 사례로 증명되었다. 그렇다면 정보보호 관리체계 프레임워크 중 가장 광범위하게 활용되고 있는 ISO/IEC 27001과 K-ISMS에 대해 간략하게 알아보도록 하겠다.

2.2.1 ISO/ISE 27001 프레임워크

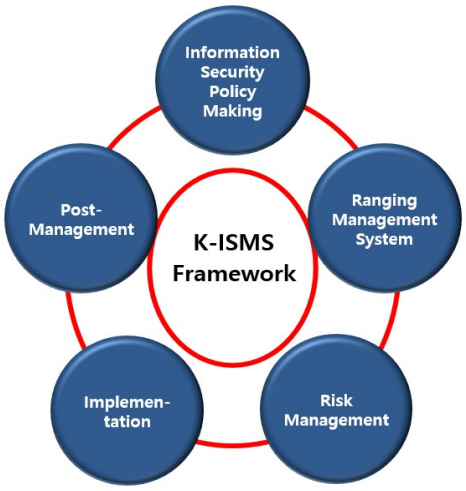
ISO/ISE 27001 프레임워크는 정보보호 관리체계에 대한 국제 표준으로서 PDGA 모델을 기반으로 한 정보보호 관리체계의 수립, 이행, 운영, 감시, 검토, 유지 및 향상을 위한 정보보안경영 인증체계이다[13]. <Table 1>과 같이 총 11개의 통제영역(정보보안 정책, 정보보호 조직, 자산관리, 인적자원 보안, 물리 및 환경적 보안, 의사소통 및 운영관리, 접근통제, 정보시스템 도입 및 개발 유지보수, 정보보호 사고 관리, 업무연속성 관리, 준거성)과 39개 통제목적, 133개 통제사항으로 구성되어 있다.

<Table 1> Classification of Control items in ISO27001

Control Domain	Items	Details
Security Policy	1	2
Organizational Security	2	11
Asset Management	2	5
Human Resources Security	3	9
Information Security Incident Management	2	5
Business Continuity Management	1	5
Compliance	3	10
Physical Security and Environmental Security	2	13
Communication and Operation Management	10	32
Access Control	7	25
Information System gain, Development and Maintenance	6	16
total	39	133

2.2.2 KISA-ISMS 프레임워크

KISA-ISMS 프레임워크는 2002년 정보통신부와 한국인터넷진흥원(KISA)에 의해 개발된 정보보호 프레임워크로서, 정보통신사업자의 보안성 강화를 주요 목적으로 하고 있다. KISA-ISMS는 ISO/ISE 27001과 같은 국제표준을 수용하면서도 국내 상황을 고려하여 설계된 정보보안 관리 표준모델이다. <Figure 1>과 같이 정보보호 관리체계를 수립, 운영하려고 하는 조직이 사용할 수 있도록 5단계 관리과정, 문서화, 그리고 <Table 2>와 같이 15개 통제영역(정보보호 정책, 정보보호 조직, 외부자 보안, 정보자산 분류, 정보보호 교육 및 훈련, 업무연속성 관리, 인적보안, 물리적 보안, 시스템 개발 보안, 암호통제, 접근통제, 운영관리, 전자거래보안, 보안사고 관리, 검토/모니터링 및 감사)로 구분된다. 각 통제영역마다 정보보호를 위해 필요한 통제목적과 이를 달성하기 위한 구체적인 통제사항이 포함된다.



<Figure 1> Certification System of K-ISMS

<Table 2> Classification of control items in K-ISMS

Control Domain	Details
Security Policy	5
Organizational Security	4
Outsiders Security	4
Classification of Information Assets	4
Education and Training	4
Human Security	5
Physical Security	12
Security of the System Development	13
Password Control	3
Access Control	14
Operations Management	22
Secure Electronic Transactions	5
Security Incident Management	7
Review, Monitor and Audit	11
Business Continuity Management	7
total	120

위와 같이 살펴본 정보보호 관리체계(ISMS)는 의무 인증 대상을 규정하고 있다.

1. ISP, IDC 사업자 및 정보통신 서비스 매출액 100억 도는 이용자 수 100만 명 이상인 사업자
2. 전년도 매출액 또는 세입 등이 1,500억 원 이상인 전체 금융회사 및 의료기관
3. 일일 평균 이용자 수 1만 명 이상인 전체 사업자

의무 인증 대상을 살펴보면 어느 정도 규모가 있는 기업들을 대상으로 하고 있는 것을 확인할 수 있다. 의무 인증 대상에서 제외되는 기업들의 경우 자율적으로 인증이 가능하게 되어 있지만 인증 비용이 만만치 않을뿐더러 인증에 소요되는 기간 역시 최소 3~4개월일 정도로 오랜 기간 신경을 써야하기 때문에 규모가 작은 기업들은 자연적으로 기피하는 현상이 발생하게 된다. 또한 통제 영역이 주로 개인정보를 취급하는 서비스 기업을 대상으로 구성되어 있어 제조업과 같은 산업기밀 보안이 필요한 기업들은 인증 자체가 무의미한 경우가 많기 때문에 이에 대한 보완이 필요하다.

2.3 정보보안 영향요인에 관한 연구

정보보안에 제대로 접근하기 위해서는 각 기업이 처한 상황과 환경에 따라 여러 가지 고려사항이 존재하고 적절한 접근 방법이 선택되어져야 한다. 하지만 기존의 연구는 정보보안의 도입 방법이나 도입 효과, 성공적인 보안 전략의 요인 탐색, 정보보안에 따른 기업 성과 등에 대한 연구가 대부분을 차지한다. 정보보안에 관련한 연구들 중 본 연구의 접근 방법과 유사한, 즉 기업이 가지고 있는 고유한 특성에 중점을 두고 정보보안에 접근했던 연구들을 정리하였다.

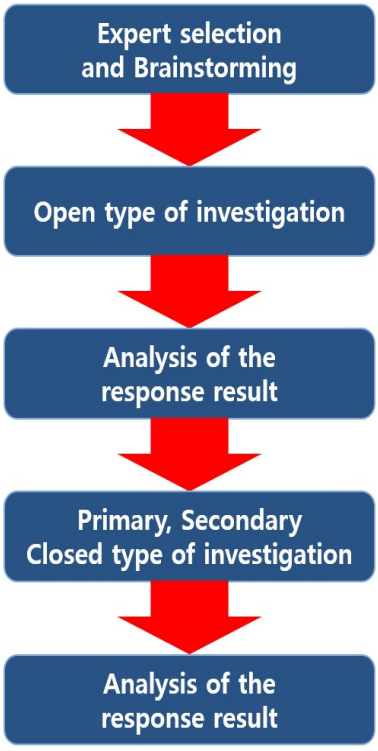
Kankanhalli et al.[14]은 정보보안을 기업에 구현할 때 고려하여야 할 요인들로 조직의 크기, 최고 경영자의 지원, 기업의 유형 등 일곱 가지 항목을 제안하면서 해당 요인들이 정보보안에 대한 관심 및 투자와 상관관계가 있음을 밝혀내었다. 그리고 정보보안에 관한 요구사항, 정보보안의 적용 및 역할은 기업에 따라 각기 다른 특징을 나타낸다고 하였다. Gorman et al.[9]은 모든 기업에 일괄적인 일반적인 보안 전략보다 보호해야 할 대상을 지정하여 관리하는 Targeted Defense가 효과적임을 주장하였다. Sherwood[34]는 기업의 비즈니스 요구사항을 분석하는 것부터 시작하여 전략을 수립하고 이에 따라 서비스를 설정한 뒤 도구를 도입하는 SALSA 모델을 제시하였다. Schneier[33]는 정보보안은 단순히 기술의 문제라기보다 조직, 개인, 사회적 요소로 구성된 하나의 사회적 시스템이라고 하였다. “정보보안은 프로세스 관점으로 접근해야 하며, 결코 솔루션으로만 해결할 수 있는 문제가 아니다.”라고 말하면서 과거부터 정보보안 분야를 지배하고 있는 기술 중심적 사고를 지적하고, 정보보안 프로세스는 실제 위협에 대해 이해를 바탕으로 초기부터 위협에 대응하는 보안정책을 만드는 것을 포함한다고 하였다. Solms and Solms[36]는 정보보안은 조직의 미션, 목표를 포함하는 전략적 맥락 속에서 수립되고 해결되어야 하는 사업부 혹은 조직적 차원의 문제라고 하였다. 정보보안은 정보자산의 안전한 환경 확보를 위해 다차원적이고 복합적인 요인을 고려해야 한다고 하였다.

Werlinger et al.[42]은 조직 내 정보보안 관리상의 중점 요인 18가지를 기술적, 인적, 조직적 관점에서 설명했다. 정보보안 전문가가 조직 내에서 직면해야 하는 기술, 사람, 조직 측면의 요인을 제시함과 동시에 이들 요인 간의 상호작용을 연구하였다. Dzazali[6]는 정보보호는 복합적이면서 동적이고 다면적인 특성을 가지고 있으므로 정보보안 이슈를 다룰 때에는 종합적인 관점에서 접근이 필요하다고 했다. Yngstrom[44]은 시스템 총괄모형은 정보보안 이슈를 다룰 때에는 종합적이고 다 학제적 사고가 필요하다고 강조했다. 왜냐하면 완벽한 보안이 바람직하고 추구해야 할 목표이지만 현실적으로 달성하기 어려운 목표이기 때문이다. Chang[4]은 정보보안은 기업의 정보화 수준에 부합하도록 그 수준과 전략을 설계해야 하므로 기업의 일반적인 정보화 계층구조를 기반으로 설계되어야 함을 전제하고서, 정보 유출 방지 활동에 특화한 중소기업 산업기술 유출방지 관리체계를 설계하였다. Kim[19]의 연구에서 기업 규모에 따라 정보자산, 위협, 취약성, 위험, 사용자 특성 등 여러 가지 정보보안 요소에 대한 사용자의 인지적 차이를 컴퓨터 바이러스를 대상으로 분석하였다. 결과적으로 먼저 보안 위협과 위험인지를 제외한 다른 연구 개념들은 기업규모에 따라 보안요소의 유의한 차이가 있는 것을 확인하였다.

3. 연구방법

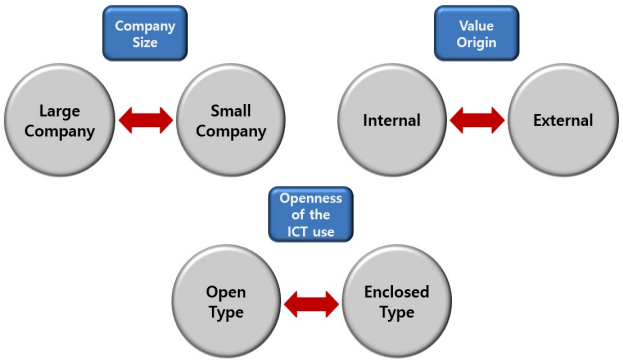
본 연구의 목적은 정보보안에 접근하고자 하는 기업의 상황에 맞는 전략 유형 프레임워크를 제시하는데 있다. 이 프레임워크는 기업의 유형을 8가지로 분류하는데, 각 기업은 자사가 속한 유형에 따라 정보보안 전략 수립 의사결정을 지원 받을 수 있다. 기업의 유형을 분류하기 위한 프레임워크 개발 방법은 <Figure 2>와 같다. 우선 보안관련 전문가 12명과 브레인스토밍을 진행하고 선행연구를 바탕으로 기업의 정보보안에 영향을 미칠 수 있다고 검증된 요인 가운데 양극의 영향 요인 3가지를 선정하였다. 그리고 각각의 요인 별로 세부 척도 항목을 다시 29명의 보안 관련 전문가를 대상으로 델파이(Delphi) 기법을 활용하여 개발한 후 SPSS 분석을 통해 구성 요인의 내용타당도 및 신뢰도를 검증하여 최종 평가 항목을 도출하였다.

가장 먼저 보안관련 전문가 12인을 선정하였는데, 브레인스토밍과 1차 개방형 조사에 참여한 보안 관련 전문가는 해당 분야에서 최소 5년 이상 근무한 팀장급 이상을 대상으로 의도적 표집(Purposive Sampling)을 통하여 12명을 선정하여 진행하였다. 브레인스토밍을 통해 기업



<Figure 2> Study Procedure

정보보안 도입 시 가장 우선적으로 고려해야 할 영향요인 3가지로 기업의 규모, 정보의 원천, ICT의 개방성 여부를 선정하여 양극의 요인으로 나누었다. <Figure 3>과 같이 '기업의 규모가 크다/작다', '정보의 원천이 내부에 있다/외부에 있다', 'ICT의 개방성 여부가 개방적이다/폐쇄적이다' 로 표현된다.



<Figure 3> The Impact Factor of the Anode of the Three

다음으로 기존에 연구되었던 정보보안 관련 선행연구와 정보보호 관리체계 프레임 워크 등에서 추출한 지표, 그리고 1차 개방형 설문 조사를 통해 얻어낸 지표들을 합산하여 3가지 척도에 해당하는 의미를 가진 후보지표 47개를 <Table 3>과 같이 선정하였다.

<Table 3> Evaluation Index Candidates

Domain	Candidate indicators	Total
Company Size	Firm age, number of employees, Total sales, Information and communication service-related sales, The average daily number of visitors for the past three months, Use pc number, Performance human resources information systems management business	7
Value Origin	Collection of personal information, Retention of other companies and partners personal information, Big data utilization, Collection of IP information, Retained personal information utilization, Trade secret, Industrial secrets, Technical standard holdings, Advantage technology compared to competitors, Ensure plan protected, The presence of the drawing and the core document, The proportion of research compared to all employees, Intellectual property right, Technology development capabilities, Form of the main products(Manufacturing/services), 6 whether large high-tech industry, Classification and definition of core human resources, The proportion of R&D investment to net sales, Whether legal protection such as patents and trade secret protection exists	19
Openness of the ICT use	Whether security specialist organization exists, Physical equipment separation on the network, Firewall, Encryption of network, Intrusion detection system, File management system, Manage the use of the PC in the network connection, Information access restriction, Allow remote work, Password management system, External connection user authentication, Whether the cooperation and co-development, Take advantage of business environment information system, Use of network equipment, The operation of the server number, Online financial transactions and business data exchange, Utilization of the information system, The intended use of the information system, Outsourcing of information systems management, Use of electronic approval and e-commerce	20

선정된 평가지표 후보군에 대한 수정 델파이 기법의 3차 라운드에 걸친 폐쇄형, 선택형 질문을 통해 각 항목의 필요성 및 중요도에 대해 분석하고 생성된 이론을 토대로 전문가들의 합의를 도출하였다.

4. 연구결과

4.1 제1라운드 평가

제1라운드 델파이 조사는 전문가 집단을 대상으로 기존의 선행연구 및 문헌분석을 통해 도출된 후보평가지표들을 대상으로 5점 리커트 척도를 이용하여 각 지표에 대한 필요성(1 = 매우 낮음, 5 = 매우 높음)을 평가하는 것이다. 기존에 도출된 후보평가지표 이외에 주관식 입력란을 따로 만들어서 전문가 집단이 추가로 필요하다고 생각하는 지표가 있다면 제시할 수 있도록 하였고, 최종적으로 47개의 후보평가지표가 만들어졌다.

최종 후보평가지표를 대상으로 한 분석결과, '기술 개발 역량' 등 5개 후보평가지표는 평균값이 2.50 미만으로 나타나 제거되었으며, 전문가의 의견에 의하여 '온라인 금융거래 및 업무자료 교환'이 '전자거래 및 전자상거래 사용여부'와 유사한 의미를 가지고 있다고 하여 하나로 통합되었다. 제1차 델파이 조사의 결과로 <Table 4>와 같이 기업의 규모 분야에 '업력'을 비롯한 7개, 가치의 근원 분야에 17개, ICT 사용의 개방성 여부에 16개가 평가지표로 도출되었다.

<Table 4> The Number of Primary and Secondary Delphi Survey Analysis Items

Domain	Number of candidate indicators of evaluation	The number of obtained evaluation index in the primary study	The number of obtained evaluation index in the second survey
Company Size	7	7	7
Value Origin	19	17	15
Openness of the ICT use	20	16	16

4.2 제2라운드 평가

제2차 델파이 조사에서는 1차 델파이 조사결과를 바탕으로 도출되었던 총 40개의 평가지표들을 대상으로 5점 리커트 척도를 활용한 폐쇄형 설문으로 작성, 각 평가지표별 중요성을 전문가들에게 질문하는 방법으로 조사하였다. 2차 델파이 조사에는 기존의 전문가 12명에 17명이 더 추가되어 총 29명의 전문가가 설문에 참여하였다. 29명의 전문가들은 보안관제, 아키텍트, 보안컨설팅 등 보안과 관련된 업무에 종사하며 1차와 마찬가지로 해당 분야 경력 5년 이상, 팀장급 이상으로 구성되었다. 2차 분석 결과, 평가지표들이 대체적으로 2.50 이상의 평균값을 나타내었는데, 가치의 근원 분야의 '영업비밀', '산업기밀' 지표가 같은 도메인의 다른 지표들과 유사하다고 의견을 제시한 전문가들에 의해 다른 지표와 통합 및 삭제되어 가치의 근원 분야의 지표는 15개로 감소하였다. 제1라운드와 제2라운드 평가를 마치고 제거 및 통합된 결과는 다음 <Table 5>와 같다. (1x)는 1라운드, (2x)는 2라운드 평가 결과 제거된 지표이고, (3x)는 3라운드에 앞서 추가로 제거된 지표이다.

<Table 5> Primary, Secondary, as a Result of the Delphi Survey Analysis

Domain	Candidate indicators	Primary need	Secondary importance
Company Size	Firm age	3.67	3.81
	number of employees	4.62	4.59
	Total sales	4.54	4.55
	Information and communication service-related sales	3.88	3.76
	The average daily number of visitors for the past three months	4.23	4.04
	Use pc number	3.06	3.25
	Performance human resources information systems management business	3.32	3.42
Value Origin	Collection of personal information	3.89	3.76
	Retention of other companies and partners personal information	4.12	4.08
	Big data utilization	2.84	3.04
	Collection of ip information(1x)	1.94	-
	Retained personal information utilization	4.05	3.89
	Trade secret(2x)	3.57	-
	Industrial secrets(2x)	3.62	-
	Technical standard holdings	4.03	3.88
	Advantage technology compared to competitors(3x)	2.78	2.82
	Ensure plan protected(3x)	3.06	2.91
	The presence of the drawing and the core document	3.21	3.62
	The proportion of research compared to all employees	3.16	3.36
	Intellectual property right	2.87	3.07
	Technology development capabilities(1x)	2.28	-
	Form of the main products(Manufacturing/services)	4.87	4.82
	6 whether large high-tech industry	3.22	3.13
	Classification and definition of core human resources(3x)	3.28	2.98
	The proportion of R&D investment to net sales	2.97	3.04
	Whether legal protection such as patents and trade secret protection exists	3.12	3.56
Openness of the ICT use	Whether security specialist organization exists	3.69	3.82
	Physical equipment separation on the network	3.76	4.04
	Firewall	4.01	3.87
	Encryption of network	4.66	4.29
	Intrusion detection system	4.16	4.18
	File management system(1x)	2.33	-
	Manage the use of the PC in the network connection	3.56	3.54
	Information access restriction	3.78	3.65
	Allow remote work	3.51	3.32
	Password management system	2.93	3.06
	External connection user authentication	3.31	3.24
	Whether the cooperation and co-development(1x)	1.95	-
	Take advantage of business environment information system	4.02	3.86
	Use of network equipment	3.84	4.07
	The operation of the server number	4.09	3.88
	Online financial transactions and business data exchange(1x)	-	-
	Utilization of the information system	3.68	3.78
	The intended use of the information system	4.14	4.13
	Outsourcing of information systems management(1x)	2.31	-
	Use of electronic approval and e-commerce	4.43	4.31

* (1x) : Variable that has been excluded from the secondary Delphi survey.
(2x) : Variable that has been excluded from the third-order Delphi survey.

4.3 제3라운드 평가

제 3차 델파이 분석을 위하여 제 2차 델파이 분석 결과 중 중요도 평균값이 2.50을 넘는 40개 지표를 가지고 리커트 5점 척도를 이용하여 지표별 중요도를 측정하는 설문을 실시하였다. 제 3차 델파이 조사에서 수렴된 평가지표에 대한 조사는 각 평가지표에 대한 중요도 검증차원에서 최종적으로 수행하였으며, 평가 결과 평균값이 3.00 미만인 평가지표(경쟁자 대비 우위 기술 확보 여부, 확보 예정 기술 여부, 핵심 인력에 대한 정의와 분류)들을 제거함으로써 제 2차 델파이 조사의 평가지표 도출과정보다 엄격하게 최종 평가지표를 도출하고자 하였다. 3차 분석 역시 2차와 동일한 29명의 전문가들이 조사에 참여하였으며, 수집된 결과를 SPSS 18.0 for Window 패키지를 사용하여 내용 타당도 비율(CVR : Content Validity Ratio)을 통해 검증하였고, 항목의 신뢰도는 항목한 일치정도를 추정하기 위하여 Cronbach's α값 계수를 산출하였다.

그 결과, <Table 6>과 같이 제 3차 델파이 조사에서는 분석에 사용된 36개의 평가지표 모두 CVR의 비율이 0.40~1.00사이의 범위에 있으므로 기업 유형 분류를 위한 평가지표로서의 내용 타당도가 있는 것으로 확인되었고, Cronbach's α 값 역시 평가지표 대부분이 0.800 이상으로 신뢰도에도 문제가 없는 것으로 분석되었다.

<Table 6> 3-Order Delphi Results Analysis

Domain	Evaluation index	CVR	Cronbach's α
Company Size	Firm age	0.76	0.88
	number of employees	0.82	0.92
	Total sales	0.85	0.9
	Information and communication service-related sales	0.77	0.83
	The average daily number of visitors for the past three months	0.83	0.81
	Use pc number	0.92	0.89
	Performance human resources information systems management business	0.88	0.83
Value Origin	Collection of personal information	0.89	0.84
	Retention of other companies and partners personal information	0.72	0.85
	Big data utilization	0.82	0.87
	Retained personal information utilization	0.85	0.92
	Technical standard holdings	0.89	0.85
	The presence of the drawing and the core document	0.81	0.82
	The proportion of research compared to all employees	0.84	0.85
	Intellectual property right	0.87	0.76
	Form of the main products(Manufacturing/services)	0.78	0.77
	6 whether large high-tech industry	0.76	0.72
	The proportion of R&D investment to net sales	0.82	0.87
	Whether legal protection	0.91	0.88
	such as patents and trade secret protection exists	0.87	0.89
Openness of the ICT use	Whether security specialist organization exists	0.52	0.88
	Physical equipment separation on the network	0.83	0.91
	Firewall	0.56	0.83
	Encryption of network	0.65	0.89
	Intrusion detection system	0.75	0.94
	Manage the use of the PC in the network connection	0.59	0.88
	Information access restriction	0.45	0.91
	Allow remote work	0.72	0.83
	Password management system	0.57	0.82
	External connection user authentication	0.63	0.92
	Take advantage of business environment information system	0.59	0.88
	Use of network equipment	0.45	0.85
	The operation of the server number	0.49	0.81
	Utilization of the information system	0.66	0.85
	The intended use of the information system	0.78	0.90
	Use of electronic approval and e-commerce	0.54	0.88

4.4 평가 종합

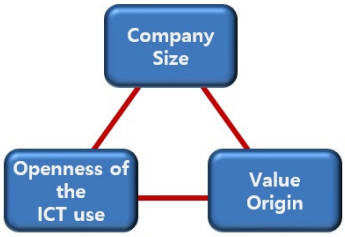
총 3라운드에 걸친 델파이 조사를 수행하는 동안 후보 평가지표 46개 중에서 11개의 지표들을 제거하고, 최종적으로 36개의 평가지표를 도출하였다. 각 분야별로 살펴보면 <Table 7>과 같이 기업의 규모 분야에서 '업력'을 비롯한 7개, 정보의 원천 분야에서 '개인정보 수집'을 비롯한 13개, ICT 사용의 개방성 분야에서 '보안 전담 조직 존재 여부' 등 16개가 도출되었다.

<Table 7> The Final Evaluation Index

Domain	Evaluation index	Total
Company Size	Firm age, number of employees, Total sales, Information and communication service-related sales, The average daily number of visitors for the past three months, Use pc number, Performance human resources information systems management business	7
Value Origin	Collection of personal information, Retention of other companies and partners personal information, Big data utilization, Retained personal information utilization, Technical standard holdings, The presence of the drawing and the core document, The proportion of research compared to all employees, Intellectual property right, Form of the main products(Manufacturing/services), 6 whether large high-tech industry, The proportion of R&D investment to net sales, Whether legal protection, such as patents and trade secret protection exists	13
Openness of the ICT use	Whether security specialist organization exists, Physical equipment separation on the network, Firewall, Encryption of network, Intrusion detection system, Manage the use of the PC in the network connection, Information access restriction, Allow remote work, Password management system, External connection user authentication, Take advantage of business environment information system, Use of network equipment, The operation of the server number, Utilization of the information system, The intended use of the information system, Use of electronic approval and e-commerce	16

정보보안을 도입하는 기업이 본 연구에서 제시하는 36개의 지표에 모두 해당될 수는 없다. 다만, 해당되는 지표를 선택하고 해당되지 않는 지표들은 제거하다보면 자신의 기업이 어떤 유형에 속하게 되는지 인식이 가능한데, 무분별하게 정보보안 솔루션 업체에 의지하고 일괄적으로 인증 체계를 따라가기 보다는, 현재 우리 기업이 어떠한 환경에 둘러싸여 있고 보호해야 할 정보 자산이 어떤 것인지 정확한 인지를 통해 정보보안에 접근하는 자세가 필요하다.

5. 정보보호 관점 기업 유형 분류 프레임워크



<Figure 4> Type of Companies Classification Framework

본 연구는 '기업의 유형을 분류하기 위해 정보보호 관점에서 어떠한 요인을 주의 깊게 살펴봐야 하는가?'라는 질문의 답을 조직의 구성요소를 토대로 모색해가는 과정이다. 이를 위해 가장 기본적인 기준이 될 3가지의 도메인을 앞서 <Figure 4>와 같이 선정하였고 그 아래 하부요인 36가지 지표를 델파이 분석을 통해 도출하였다. 제시된 프레임워크를 사용하여 각자 기업이 속하는 유형을 찾는 방법은 어렵지 않다. 각 도메인별로 구성된 지표를 기업에 하나씩 적용시켜가면서 더 많은 해당사항이 있는 곳에 표시를 한 후 다음 도메인으로 넘어가면 된다. 그렇다면 프레임워크를 통해 도출될 기업의 유형에는 어떤 것들이 있고 특징지을만한 사항은 무엇인지 알아보고자 한다.

유형 1은 기업의 규모가 크고 정보의 원천이 내부에 있으며 폐쇄적인 ICT 사용 환경을 가지고 있는 기업이다. 해당 유형의 경우 규모가 크기 때문에 보유한 정보자산의 가치도 큰 경우가 많다. 또한 보안에도 전담부서를 가지고 있을 가능성이 높은데, 이런 유형은 내부자 보안, 특히 막대한 금전적 이득을 노리고 고의로 유출하는 경우가 대부분이다. 제조업에서 많이 발생하며 2014년 LG전자의 로봇청소기 핵심기술 유출이나 현대자동차의 신차 개발 도면 유출 사건 등이 대표적이다.

유형 2는 유형 1과 마찬가지로 내부 정보 자산의 가치가 큰 경우인데 상대적으로 보안에 많은 투자를 하지 않았거나 특정 부분에만 신경을 쓴 경우이다. 대표적으로 공공기관이 많이 해당된다. 지난 2015년 경기도 산하의 공공기관 26곳이 23% 정도의 정보보안 수준을 보여 문제가 된 적이 있었다. 기업의 이미지가 수익과 직접적인 연관이 없으며 기관장이 수시로 바뀌기 때문에 정보보안 분야까지 대체로 신경 쓰지 않는 경우가 많다.

유형 3은 기업의 규모가 크고 정보의 원천이 외부에 있으며 폐쇄적인 ICT 사용 환경을 가지고 있는 기업이다. 대표적으로 대학교나 골프장 같은 개인정보를 취급하지만 누구나 접근 가능한 환경은 아닌 곳이 해당된다. 2011년 충북소재 사립 대학교에서 일어난 해킹 사건이나

2012년, 2014년에 각각 130만, 20만건의 회원정보가 유출된 사고사례가 있다.

유형 4는 기업의 규모가 크고 정보의 원천이 외부에 있으며 개방적인 ICT 사용 환경을 가지고 있는 기업이다. 개인정보 피해가 가장 많이 발생하는 유형으로 각종 카드사의 개인정보 유출 사건, 2011년 SK컴즈의 3,500만 개인정보 유출 사건 등 뉴스에도 자주 등장하는 사고사례가 여기에 해당된다.

유형 5는 기업의 규모가 작고 정보의 원천이 내부에 있으며 폐쇄적인 ICT 사용 환경을 가지고 있는 기업이다. 이제 막 시작한 중소 제조업이 많이 해당되는 유형이다. 정보보안 정책은 물론이고 담당 부서조차 없는 경우가 많으며 정보보안이라는 개념 자체에 무감각하다. 초기에 정보 자산이 없을 때는 상관없지만 규모가 커질수록 위험해지므로 운영진에서 대비를 해야 한다. 다년간에 걸쳐 정부 지원 등으로 어렵게 개발한 기술이 한순간에 도난당하는 사고사례가 빈번하게 일어나는 유형. 2013년 삼성 협력업체 A사가 국가지원을 받아 개발한 국책기술 도면 유출 사고가 대표적이다.

유형 6은 기업의 규모가 작고 정보의 원천이 내부에 있으며 개방적인 ICT 환경을 가지고 있는 기업이다. 유형 5와 약간 다르게 정보시스템을 이용한 연구개발을 하는 중소 제조업이 여기에 해당한다. 전자문서의 형태로 산업기밀을 보관하는 경우가 많으며 이메일, 외장하드 등으로 사고가 발생한다. 2014년 100억 원대의 인쇄회로기판 핵심기술을 USB로 도난당한 사고가 있었다.

유형 7은 기업 규모가 작고 정보의 원천이 외부에 있으며 폐쇄적인 ICT 사용 환경을 가지고 있는 기업이다. 대리운전 업체, ATM기기 하드디스크 복제, 포스 단말기 정보 유출처럼 온라인이 아닌 오프라인으로 사고가 발생하는 경우가 많다.

유형 8은 기업 규모가 작고 정보의 원천이 외부에 있으며 개방적인 ICT 사용 환경을 가지고 있는 기업이다. 유형 5와 비슷하지만 개인정보를 주로 취급하는 이제 막 시작한 온라인 쇼핑몰 같은 경우가 여기에 해당된다. 하지만 유형 5와 마찬가지로 회원 수가 늘어나게 되면 자연스럽게 정보자산의 크기도 커지기 때문에 이에 따른 대비가 필요한 유형이다.

6. 결 론

2015년 국가정보원 산업기밀보호센터에서 발표한 자료에 따르면 2010년부터 2014년까지 5년간 총 229건의 산업기밀 유출 피해 중 중소기업에서 발생한 경우가 전체의 64%를 차지하여 대기업의 16%와 비교했을 때 현저한 차이를 보였다. 또한 피해가 발생한 중소기업의 절반정도는 2회 이상 반복하여 피해가 발생한 것으로 나타났다. 2015년 정보보호 실태조사에 따르면 조사에 응답한 7,089개의 기업들 중 약 18%에 해당하는 1,270여개 기업에서 정보보호 예산을 편성하지 않은 이유로 '정보보호를 어떻게 해야 하는 모름'이라고 답변하였다. 또한 이 수치는 규모가 작은 기업일수록 더욱 크게 나타난 것으로 조사되었다. 조사 그대로 대다수의 기업들은 정보보안에 대해 신경 쓸 여력이 거의 없으며, 설령 있다 하더라도 접근 방법에 대해 제대로 알지 못하는 경우가 많다고 볼 수 있다. 현재 정보보안에 접근할 때 모든 기업이 일관적이고 단편적인 접근 방법을 사용하는 것은 이미 많은 보안사고 사례를 통해 알 수 있듯이 효율적인 방법이 아니다. 이는 정보보안 자체의 성격이 복합적이고 다면적이며 동적인 특징을 가지고 있기 때문이기도 하며, 개별 기업이 가지고 있는 성격이나 당면해 있는 환경 또는 상황 또한 매우 많은 다양성을 지니고 있기 때문이다.

본 연구는 이러한 다양성을 고려하여 정보보안에 접근하고자 하는 기업의 의사결정에 도움을 줄 수 있는 보다 현실적인 기여를 하고자 진행되었다. 평가지표에 대한 보완의 필요성을 느끼며, 향후 기업 유형에 따른 실제 사고 사례와 성공적인 대응 방안에 대해 연구하여 보다 효과적인 개선방안 제시가 필요하다.

References

[1] Bharadwaj, A., Keil, M., and Mahring, M., Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, 2009, Vol. 18, No. 2, pp. 66-79.

[2] Brancheau, J.C., Janz, B.D., and Wetherbe, J.C., Key Issues in Information Systems Management : 1994-95 SIM Delphi Results, *MIS Quarterly*, 1996, Vol. 20, No. 2, pp. 225-242.

[3] Calder, A. and Van Bom, J., Implementing Information Security Based on ISO 27001/ISO 17799, Van Haren Publishing, 2006.

[4] Chang, H.B., The Design of Information Security Management System for SMEs Industry Technique Leakage Prevention, *Korea Multimedia Society*, 2010, Vol. 13 No. 1, pp. 111-121.

[5] Doherty, N.F. and Fulford, H., Do Information Security Policies Reduce the Incidence of Security Breaches : An Exploratory Analysis, *Information Resources Management Journal*, 2005, Vol. 4, pp. 21-38.

[6] Dzazali, S. and Zolait, A.H., Assessment of Information

Security Maturity : an Exploration Study of Malaysian Public Service Organizations, *Journal of Systems and Information Technology*, 2012, Vol. 14, No. 1, pp. 23-57.

[7] Ettredge, M. and Richardson, V.J., Information Transfer among Internet Firms : the Case of Hacker Attacks, *Journal of Information Systems*, 2003, Vol. 17, No. 2, pp. 71-82.

[8] Flint, D.J., Woodruff, R.B., and Gardial, S.F., Exploring the Phenomenon of Customers Desired Value Change in a Business to Business Context, *Journal of Marketing*, 2002, Vol. 66, No. 4, pp. 102-117.

[9] Gorman et al., Least Effort Strategies for Cybersecurity, *The Critical Infrastructure Project Workshop I : Working Papers*, May 2003, pp. 1-14.

[10] Hagen, J.M., Albrechtsen, E., and Hovden, J., Implementation and Effectiveness of Organizational Information Security Measures, *Information Management and Computer Security*, 2008, Vol. 16, No. 4, pp. 377-397.

[11] Hawkins, S. and Yen, D.C., Awareness and Challenges of Internet Security, *Information Management and Computer Security*, 2000, Vol. 8, No. 3, pp. 131-143.

[12] Hu, Q., Hart, P., and Cooke, D., The Role of External and Internal Influences on Information Systems Security Practices : An Institutional Perspective, *The Journal of Strategic Information Systems Archive*, 2006, Vol. 16, No. 2, pp. 153-172.

[13] Introduction to privacy and personal information management framework, Financial Security Institute, 2011.

[14] Kankanhalli et al., An Integrative Study of Information Systems Security Effectiveness, *Journal of Information Management*, 2003, Vol. 23, No. 2, pp. 139-154.

[15] Karyda, M., Kiountouzis, E., and Kokolakis, S., Information security policies : a contextual perspective, *Computers and Security*, 2005, pp. 246-260.

[16] Kast, F.E. and Rosenzweig, J.E., General Systems Theory : Applications for Organization and Management, *Academy of Management Journal*, 1972, Vol. 15, No. 4, pp. 447-465.

[17] Katz, D. and Kahn, R.L., The Social Psychology of Organizations(2nd ed.). *New York : Wiley*, 1978.

[18] Kim et al., The Effects of Information Security Policies, Security Controls and User's Characteristics on Anti-Virus Security Effectiveness, *Journal of Information Systems*, 2006, Vol. 15 No. 1, pp. 145-168.

[19] Kim, H.O. and Baek, D.H., A Study on Categorization of Accident Pattern for Organization's Information Security Strategy Establish, *Journal of the Society of Korea Industrial and Systems Engineering*, 2015, Vol. 38 No. 4, pp. 193-201.

[20] Kim, M.S., Jeoune, D.S., Nam, K.H., Kim, G.R., and Han, C.M., Implication of Industrial Security Capacity Based on Level Evaluation, *The Korean Society for Quality Management*, 2013, Vol. 41, No. 4, pp. 649-658.

[21] Korea Communications Commission Report, A Fact-Finding on Leak Out of Personal Data, KCC, 2015.

[22] Lohmeyer, D.F., McCrory, J., and Pogreb, S., Managing Information Security, The McKinsey Quarterly, Special Edition : Risk and Resilience, 2002, Vol. 2, pp. 12-16.

[23] Mckelvey, B. and Aldrich, H., Populations, Natural Selection, and Applied Organizational Science, *Administrative Science Quarterly*, 1983, Vol. 28, No, 1, pp. 101-128.

[24] Miller, P., Strategic Industrial Relations and Human Resource Management-Distiction, Definition and Recognition, *Journal of Management Studies*, 1987, Vol. 24, No. 4, pp. 347-361.

[25] Mintzberg, H., The design school : Reconsidering the basic premises of strategic management, *Strategic Management Journal*, 1990, Vol. 11, No. 3, pp. 171-195.

[26] Morgan, R.T., Image of organization. Sage Publications, 1986.

[27] National Defense Science and Technology Vocabulary, 2011.

[28] Pfhleeger, C.P., Security in Computing, Second edn, Prentice Hall, United States of America, 1997.

[29] Phares, E.J., Introduction to personality, Columbus, OH : Carles E. Merrill, 1984.

[30] Rich, P., The Organizational Taxionomy : Definition and Design, *Academy of Management Review*, 1992, Vol. 17, No. 4, pp. 758-781.

[31] Sanchez, J.C., The Long and Thorny way to an Organizational Taxonomy, *Organization Studies*, 1993, 14/1: 73-92.

[32] Sarker, S., Lau, F., and Sahay, S., Using an Adapted Grounded Theory Approach for Inductive Theory Building About Virtual Team Development, *DATA BASE for Advances in Information Systems*, 2001, Vol. 2, No. 1, pp. 38-56.

[33] Schneier, B., Secrets & Lies-Digital Security in a Networked World, *Wiley Computer Publishing*, New York, 2002.

[34] Sherwood, J., SALSA : A Method for Developing the Enterprise Security Architecture and Strategy, *Computers and Security*, 1996, Vol. 15, Issue. 6, pp. 501-506.

[35] Smith, E., Kritzinger, E., Oosthuizen, H.J., and Von Solms, S.H., Information Security Education, in Proceedings of

the WISE 4 Conference, Moscow, Russia, 2004.

[36] Solms, V. and Solms, R., The 10 Deadly Sins of Information Security Management, *Computers and Security*, 2004, Vol. 23, No. 5, pp. 371-376.

[37] Spears, J.L. and Barki, H., User Participation in Information Systems Security Risk Management, *MIS Quarterly*, 2010, pp. 503-522.

[38] Survey of personal information, *Ministry of Science, ICT and Future Planning*, 2015.

[39] Thomson, M.E. and Von Solms, R., Information Security Awareness : Educating Your Users Effectively, *Information Management and Computer Security*, 1998, Vol. 6, No. 4, pp. 167-173.

[40] Von Solms, R. and Von Solms, S.H., From policies to culture, *Computers and Security*, 2004, Vol. 23, No. 4, pp. 275-279.

[41] Von Solms, S.H., Information Security Management through Measurement, in Proceedings of the SEC99 conference, Johannesburg, South-Africa, 1999.

[42] Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K., Preparation, detection, and analysis : the diagnostic work of IT security incident response, *Information Management and Computer Security*, 2010, Vol. 18, No. 1, pp. 26-42.

[43] Wood, C.C., Why Information Security is Now Multi-Disciplinary, Multi-Departmental, and Multi-Organizational in Nature. *Computer Fraud and Security*, 2004, No. 1, pp. 16-17.

[44] Yngstrom, L., A Systemic-Holistic Approach to Academic Programmes in IT Security, *Ph.D Thesis, Department of Computer and Systems Sciences*, University of Stockholm and the Royal Institute of Technology, 1996.

ORCID

Hee Ohl Kim | http://orcid.org/0000-0001-8600-4528

Dong Hyun Baek | http://orcid.org/0000-0002-3107-9511