Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.919

정보보호관리체계(ISMS) 항목의 중요도 인식과 투자의 우선순위 비교 연구

이 중 정,[1†] 김 진,[2] 이 충 훈[1‡]
[1]연세대학교 정보대학원, [2]삼정 KPMG

A comparative study on the priorities between perceived importance and investment of the areas for Information Security Management System

Choong-Cheang Lee,[1†] Jin Kim,[2] Chung-hun Lee[1‡]
[1]Graduate School of Information, Yonsei University, [2]Samjong KPMG

요 약

최근의 개인정보 유출과 같은 정보보안 사고들이 기업의 매출 감소와 이미지 손실에 직접적인 영향을 주는 심각한 위험 관리 요소가 됨에 따라 체계적인 정보보호 관리를 위해 정보보호관리체계를 도입하는 기업들이 증가하고 있다. 그러나 기업 내 정보보호 인식과 달리 적은 투자로 인해, 한정된 예산으로 다양한 정보보호 요소들을 효과적으로 관리할 수 있는 방안이 중요해지고 있다. 본 연구에서는 정보보호관리체계의 13개 항목들에 대해 정보보호전문가들의 중요도 평가를 통해 우선순위를 도출하여, 단계적으로 정보보호관리체계를 구축할 수 있는 방향을 제공한다. 그리고 각 항목들에 대한 투자 정도도 평가하여 중요도와 투자 간의 우선순위 차이를 비교·분석하였다. 연구 결과 침해사고 관리가 가장 중요한 것으로 나타났으며, 투자 정도에서는 IT 재해복구가 가장 높은 것으로 확인되었다. 그리고 정보보호 중요도와 투자 간의 우선순위 차이가 큰 정보보호 항목은 암호통제, 정보보호정책, 정보보호교육, 인적보안으로 확인되었다. 본 연구 결과는 정보보호관리체계 도입을 고려하거나 운영 중인 기업들이 한정된 예산을 고려하여 효과적인 정보보호 투자에 대한 의사결정 자료로 활용될 수 있을 것으로 기대한다.

ABSTRACT

Recently, organizational efforts to adopt ISMS(Information Security Management System) have been increasingly mandated and demanded due to the rising threat and the heavier cost of security failure. However there is a serious gap between awareness and investment of information security in a company, hence it is very important for the company to control effectively a variety of information security threats within a tight budget. To phase the ISMS, this study suggests the priorities based on evaluating the Importance of 13 areas for the ISMS by the information security experts and then we attempt to see the difference between importance and investment through the assessment of the actual investment in each area. The research findings show that intrusion incident handling is most important and IT disaster recovery is the area that is invested the most. Then, information security areas with the considerable difference between priorities of importance and investment are cryptography control, information security policies, education and training on information security and personnel security. The study results are expected to be used in making a decision for the effective investment of information security when companies with a limited budget are considering to introduce ISMS or operating it.

Keywords: Information Security Management System, Information Security Priorities, Information Security Importance, Information Security Investment

접수일(2014년 6월 20일), 수정일(2014년 9월 22일), 게재확정일(2014년 9월 22일)

† 주저자, cclee@yonsei.ac.kr
‡ 교신저자, goguming@gmail.com(Corresponding author)

I. 서 론

오늘날 정보보호는 기업들에게 중요한 경영관리 요소 중에 하나이다. 최근의 개인정보 유출사고에서 볼 수 있듯이 한 기업의 보안 사고는 기존고객의 이탈뿐만 아니라 매출감소, 기업 이미지 손실까지 초래하는 심각한 위험 관리 요소가 되고 있다. 이러한 사회적 변화에 따라 정보보호 중요성에 대한 기업의 인식 수준이 높아졌으며, 체계적인 정보보호 관리를 위해 정보보호관리체계를 도입하는 기업이 증가하고 있다.

하지만 기업들의 정보보호 투자는 인식만큼 증가하고 있지 않다. 2012년 한 해 동안 정보화 예산의 일부를 정보보호에 투자한 사업체는 19.2% 증가했지만, 정보화 예산 중 5% 이상 정보보호관련 분야에 지출한 사업체는 3.2%로 매우 미흡한 것으로 조사되었다[9].

따라서 한정된 예산으로 수많은 정보보호 요소들을 효과적으로 관리하기 위해서는 정보보호관리체계의 주요 항목들에 대한 중요도 인식을 바탕으로 우선순위를 도출하여, 단계적으로 정보보호관리체계를 수립하는 것이 중요하다. 그리고 대기업에 비해 정보보호관련 투자 자원이 상대적으로 제한적일 수 밖에 없는 중소기업에게는 정보보호 중요도를 바탕으로 선택과 집중을 통한 투자·관리가 무엇보다 중요하다고 할 수 있다. 또한 연구개발, 기술, 정책 등 다양한 분야의 선행연구들에서도 효과적인 성과를 위해 우선순위를 고려한 투자의 중요성을 강조하고 있다[1,6,11].

그러나 정보보호 우선순위에 관한 선행연구들은 산업보안, Big data 등과 같은 특정분야에 한정되어 있어서 국내 모든 기업에 공통적으로 적용하는데 한계가 있다[2,12].

본 연구에서는 기업들이 정보보호관리체계 도입 시, 국내 표준 역할을 하고 있는 한국인터넷진흥원의 ISMS(Information Security Management System) 13개 정보보호대책 항목을 기반으로 정보보호전문가의 중요도 평가를 통해 우선순위를 도출하고자 한다. 그리고 각 항목들에 대한 투자 정도도 평가하여 중요도와 투자 간의 우선순위 차이를 비교·분석하고자 한다. 본 연구 결과를 바탕으로 기업들은 정보보호 항목의 중요도를 고려하여 한정된 예산을 투자함으로써, 조직의 상황에 맞게 투자 대비 효과를 높일 수 있는 정보보호관리체계를 구축할 수 있을 것이다. 그리고 정보보호 항목의 중요도와 실제 투자와의 차이 비교를 통해, 현재 정보보호관리체계를 운영하고 있는 기업들의 개선방향에 대한 주요 고려사항들을 제안할 수 있을 것으로 기대된다.

따라서 본 연구의 목적은 조직 내 정보보호관리체계를 구축 또는 운영 시 효과적인 성과를 도출하기 위해 "첫째, ISMS 인증의 13개 정보보호대책 항목들에 대한 중요도 우선순위는 어떻게 되는가?", "둘째, ISMS 인증의 13개 정보보호대책 항목들의 중요도와 투자의 우선순위에는 어떤 차이가 있는가?"를 정보보호전문가 대상의 AHP(Analytic Hierarchy Process)기법을 사용하여 확인하고자 한다.

본 논문의 구성 체계는 다음과 같다. 제1장은 서론으로 연구 배경, 연구 목적, 연구 범위 등을 기술하였으며, 제2장에서는 선행 연구 논문 및 문헌 자료를 통해 정보보호관리체계와 계층분석기법을 체계적으로 정리하였다. 제3장, 4장, 5장에서는 실증연구를 위한 분석방법과 결과를 도출하였다. 제6장에서는 본 연구 결과의 요약과 연구 결과의 시사점 및 한계점을 제시하였다.

II. 이론적 배경

2.1 정보보호관리체계

정보보호관리체계(ISMS)는 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위하여 정보보호 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리·운영하는 일련의 과정 및 활동이다. 또한 조직 내에서 운영되고 있는 정보보호관리체계를 제3자의 인증기관이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도를 정보보호관리체계 인증제도라고 한다[17].

우리나라에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 '정보보호관리체계 인증'이라는 법률적 근거를 바탕으로 연간 매출액 또는 이용자 수 등 법적 기준에 부합하는 정보통신서비스 제공자는 의무적으로 정보보호관리체계를 도입하여 인증을 받도록 되어 있다. 그리고 정보보호 안전진단 제도가 폐지되고 정보보호관리체계로 통합됨에 따라 공공기관까지 적용범위가 확대되었다.

또한 일련의 개인정보유출 사건으로 인해 정보보호에 대한 사회적 관심이 높아지고, 기업 내 지적자산에 대한 보호가 중요해짐에 따라 정보보호관리체계도입을 통한 정보보호 강화가 활성화되고 있다. 실제 정보보호관리체계 인증을 받은 업체 수가 2012년 25건에서 2013년 126건으로 급격히 증가하였다[10].

정보보호관리체계는 Table 1과 같이 13개의 정보보호대책과 92개의 통제항목으로 구성된다. 정보보호관리체계 인증 제도를 도입한 2002년 이후, ICT 및 정보보호 환경 변화에 적합하도록 통제항목들이 지속적으로 개선되었다. 그래서 정보보호관리체계는 각 조직에서 정보보호관리에 필요한 통제항목을 선택하고 각 보안 요구사항에 맞게 관리체계를 마련할 수 있는 국내 표준으로 활용되고 있다.

ISMS관련 선행연구는 조직 내 정보보호관리체계 도입 시 고려사항이나 효과성 확인에 한정되어 있다. 김지숙 등[4]은 민간기업과 공공기간의 정보보호관리체계 통제항목을 비교·연구하여 미흡한 사항을 분석하였으며, 배영식[17]은 정보보호관리체계 인증과 기업의 경영성과와의 유의적 관계를 실증적으로 증명하였다. 그리고 김기철 등[7]은 한국형 스마트 그리드를 위한 정보보호관리체계 평가 기준을 제안하였다. 하지만, 한정된 정보보호 예산을 고려하여 정보보호 통제항목들에 대한 우선순위 분석과 실제 투자와의 관계에 대한 연구는 거의 이루어지지 않았다.

Table 1. Information Security Countermeasures

Areas	Control activities
1. Information security policies	6
2. Information security organization	4
3. Security of External Parties	3
4. Information asset classification	3
5. Education and training on information security	4
6. Personnel security	5
7. Physical security	9
8. System development security	10
9. Cryptography control	2
10. Access control	14
11. Operations security	22
12. Intrusion incident handling	7
13. IT disaster recovery planning	3
Total	92

2.2 계층분석기법(AHP)

AHP(Analytic Hierarchy Process)는 의사결정 대상을 계층적으로 표현하고, 의사결정자의 판단에 기반하여 대상들에 대한 우선순위를 부여하는 의사결정 모형이다[13]. 기존의 의사결정방법으로 모델화 또는 수량화할 수 없었던 주제나 주관적인 판단을 AHP 방법을 통해 계량화할 수 있다[3,16].

AHP는 복잡한 문제를 단순화해서 합리적인 의사결정을 할 수 있도록 다수의 항목들에 대한 가중치를 동시에 고려하는 대신, 두 개씩 짝을 지어 쌍대비교(pairwise comparison)를 통해 평가 대상항목의 가중치를 도출하여 항목을 중요도에 따라 계층적으로 구조화한다[13,15].

따라서, AHP 방법은 다수의 속성 또는 평가요소들이 계층적으로 복잡하게 구성되어 있을 때 효과적으로 분석할 수 있는 유용한 도구이다.

AHP 분석 시, 최상위 계층에는 평가 목적을 두고 그 하위에는 목표에 영향을 주는 평가 기준을 둔다. 그리고 평가 기준은 여러 단계로 나누어서 세부 평가기준으로 구성할 수 있으며, 필요에 따라서 평가 기준의 하위에 평가 대안을 둘 수 있다. AHP에서 계층 구조화를 잘못하면 결과가 정확하지 않을 수 있기 때문에 계층 구분과 군집화를 통한 구조화가 중요하다.

AHP는 평가자의 응답을 바탕으로 의사결정이 이루어지므로 평가자들의 응답에 일관성이 있어야 한다. 응답에 일관성 결여될 경우 결과의 정확성이 떨어지게 된다. 그래서 이러한 오류를 방지하기 위해 일관성 비율(Consistency Ratio)을 기준으로 평가자의 응답에 일관성이 있는지를 검증한다. 일관성 비율이 10% 이내인 경우에만 판단에 일관성이 있는 것으로 간주되며, 일관성 비율이 10%를 초과하면 쌍대비교를 다시하거나 설문지를 수정해야 한다[14]. 그러나 일관성 비율이 20% 이하일 때도 일반적으로 이용될 수 있다[5].

III. 연구 모형 및 평가 기준

3.1 연구 모형

정보보호 항목의 중요도 및 투자에 대한 우선순위 평가를 위한 연구모형은 Fig.1과 같이 제1계층에는 모델의 목표, 제2계층에는 3개의 상위평가기준, 제3계층에는 13개의 하위평가기준으로 구성하였다.

하위평가기준은 조직 내에서 정보보호관리체계를 수립할 시, 국내 표준으로 활용되고 있는 ISMS 인증의 13개 정보보호대책을 적용하였으며, 상위 평가기준은 정보보호 주요 3가지 영역인 관리적 보안, 물리적 보안, 기술적 보안을 적용하여 하위평가기준을 구분하였다[8].

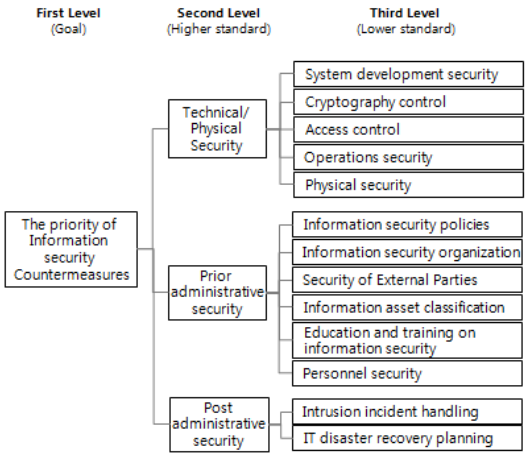

Fig. 1. Research hierarchy

ISMS의 13개의 정보보호대책 중 관리적 보안이 물리적, 기술적 보안에 비해 상대적으로 비중이 높아 채정우 등[2]의 분류 방법을 적용하여 관리적 보안을 사전 관리적 보안과 사후 관리적 보안으로 구분하였다. 그리고 물리적 보안은 1개의 정보보호대책만 적용되어 기술적 보안과 통합하여 기술적/물리적 보안으로 구분하였다.

Table 2. The evaluation criteria of research

Division	Evaluation criteria	Operational definition
Higher standard	Technical/ Physical security	Technical security area including technology, policy, process applied for information security, access control and physical security area to protect information systems, facilities and so on from environmental risk and unauthorized intrusion. (network security, PC security, access control etc.)
	Prior administrative security	Administrative security area including composition of organization, personnel recruiting, policy making to prevent security incidents. (security policy, security organization, security education)
	Post administrative security	Administrative security area to effectively deal with security incidents. (Intrusion incident handling, IT disaster recovery etc.)
Lower standard	System development security	When a new information system is developed or the existing system is changed, you should apply and understand clearly the security requirements.
	Cryptography control	Cryptography policies including encryption object, encryption strength and key management should be established and implemented.
	Access control	Access control policies should be established and implemented in order to control the unauthorized person.
	Operations security	The procedure establishment to operate information systems and their change management.
	Physical security	You should install the equipments to protect information systems after designating protection zone for them and restrict the public access to the protection area.
	Information security policies	Information security policies including security guideline and procedure should be shared all employees with CEO's approval and be renewed consistently.
	Information security organization	You should appoint CISO and organize security team. Information protection committee also is constituted to review

		the major considerations related to information security.
	Security of External Parties	When the external parties need to process your information or access your information asset, you should write up a contract including exactly security requirements.
	Information asset classification	You should identify all information assets in the organization following the classification standard and grade security level according to their importance.
	Education and training on information security	You should establish an annual educational planning and educate regularly employees and external parties.
	Personnel security	Employees who access the important information should be under control of the security manager and submit security oath.
	Intrusion incident handling	You should deal with intrusion incidents response system and conduct simulation training regularly.
	IT disaster recovery planning	You should establish IT disaster recovery planning including organization for recovery, contact list for an emergency , recovery procedures and regular simulation of recovery system.

Source: Korea Internet & Security Agency 2013

IV. 연구방법

4.1 표본 추출 및 자료 수집

정보보호 전문가 22명을 대상으로 AHP 설문조사를 진행하여 일관성 비율이 0.2를 초과하는 7부를 제외하고 15부를 분석에 활용하였다. 설문에 응답한 전문가는 정보보호 컨설턴트 7명, 기업보안관리자 7명, 정부기관보안관리자 1명이다. 최종 응답자 15명에 대한 표본의 특성은 Table 3과 같다.

Table 3. The characteristic of sample

Division	Detail	The number of re-spondent	Rate
Information security career	3~5 years	10	67%
	6~8 years	3	20%
	more than 9 years	2	13%
Role	Information security consultant	7	47%
	Information security manager in a company	7	47%
	Information security manager in a government agency	1	6%
Academic background	Bachelor´s degree	8	53%
	Master´s degree	6	40%
	Doctor´s degree	1	7%
ISMS knowledge level (overwriting available)	ISMS certification examiner	1	7%
	Learning the course of ISMS certification	10	67%
	ISMS consultant	9	60%
	Understanding 13 areas for ISMS	15	100%

4.2 AHP 분석절차

본 연구는 다음과 같은 순서로 분석을 진행하였다.

1단계: Fig.1과 같이 의사결정 문제를 계층구조로 분해한다.

2단계: 정보보호 전문가 30명에게 AHP 설문을 진행하여 22명의 설문을 회수하였으며, 설문은 같은 계층에 있는 평가기준들을 대상으로 쌍대비교 (Paired Comparison: 두 개의 항목을 서로 비교)를 통해 상대적으로 어느 항목이 더 중요한지 평가하였다.

3단계: 설문결과를 토대로 일관성 지수를 산출한 후, 무작위 지수로 나누어 일관성 지수를 도출하였다. 일관성 지수가 0.2를 초과하는 7부의 설문을 분석대상에서 제외하고 최종 15부를 가지고 중요도를 산출하였다.

4단계: AHP 기법에서 일반적으로 많이 사용되는

기하평균법을 사용하여 단일화된 데이터를 만들어 각 계층의 항목별 상대적 중요도를 산출하였다. 그리고 1계층과 2계층의 상대적 중요도를 곱하여 전체 항목에 대한 상대적 중요도를 산출하여 우선순위를 도출하였다.

5단계: 동일한 방법으로 정보보호대책 13개 항목에 대한 전문가의 소속 조직(또는 최근 컨설팅을 수행한 고객사)의 투자 배정 순위를 도출하여 중요도와 비교하였다.

V. 실증분석 결과

Table 4는 정보보호대책의 상위기준과 하위기준 간 우선순위에 대한 정보보호전문가들의 의견을 보여준다. 상위기준 간 쌍대비교 결과는 기술적/물리적 보안, 사전 관리적 보안, 사후 관리적 보안의 중요도가 각각 36%, 42.5%, 21.5%로 나타났다. 상위기준 간의 쌍대비교에서 사전 관리적 보안이 가장 중요한 것으로 확인되었다.

하위기준 간의 상대적 중요도는 기술적/물리적 보안 측면에서 접근통제가 29.3%로 가장 높게 나타났으며, 사전 관리적 보안 측면에서는 인적보안이 23.3%로 가장 중요한 것으로 평가되었다. 그리고 사후 관리적 보안 측면에서는 침해사고 관리가 54.1%로 IT 재해복구보다 더 중요한 것으로 확인되었다.

Table 4. The priority analysis of importance among information security countermeasures

Higher standard	Relative importance of higher standard	Lower standard	Relative importance of lower standard	Final relative importance	Priorities
Technical/ Physical Security	0.360	System development security	0.184 NO. 4	0.066	8
		Cryptography control	0.187 NO. 3	0.049	13
		Access control	0.293 NO. 1	0.105	2
		Operations security	0.133 NO. 5	0.066	9
		Physical security	0.202 NO. 2	0.073	6
Prior administrative security	0.425	Information security policies	0.157 NO. 3	0.067	7
		Information security organization	0.153 NO. 4	0.065	10
		Security of External Parties	0.128 NO. 5	0.054	11
		Information asset classification	0.117 NO. 6	0.050	12
		Education and training on information security	0.212 NO. 2	0.090	5
		Personnel security	0.233 NO. 1	0.099	3
Post administrative security	0.215	Intrusion incident handling	0.541 NO. 1	0.117	1
		IT disaster recovery planning	0.459 NO. 2	0.099	4

연구결과 상위기준 간 상대적 중요도에서 사전 관리적 보안이 가장 중요한 것으로 나타났다. 이러한 결과가 나온 이유는 조직 내에서 정보보호를 강화하기 위해서는 정책수립과 인력구성 등이 기본적으로 갖춰져야 하기 때문이다.

기술적/물리적 보안 측면에서는 접근통제가, 사전 관리적 보안측면에서는 인적보안이 가장 중요한 것으로 확인되었다. 이는 최근에 내부자 유출로 인해 발생한 일련의 개인정보유출 사건에 기인한 것으로 판단된다. 외부자에 비해 내부자의 경우, 중요 시스템에 대한 접근이 상대적으로 용이하기 때문에 시스템

에 대한 접근권한 관리와 관리자 식별 등에 있어서 더 엄격하고 강화된 보안이 이루어져야 한다.

사후 관리적 측면에서는 침해사고 관리가 IT 재해복구보다 상대적으로 중요하다고 확인되었다. 이러한 결과는 최근의 개인정보유출 사건들이 기업의 재무적 손실에 직접적인 영향을 주는 것으로 확인됨에 따라 개인정보 침해사고 이후 기업들의 적절한 대응관리가 피해를 최소화하는데 있어 매우 중요해졌기 때문이다.

정보보해대책 중 상위기준의 상대적 투자에서는 기술적/물리적 보안이 49.7%으로 가장 투자가 많이 이루어진 것으로 확인되었다. 이러한 결과는 법률적으로 기본적인 보안시스템 구축을 요구하고 있어 조직 내 정보시스템 구축 시 일정한 투자가 필요한 반면에 사전·사후 관리적 보안은 조직의 의사결정에 따라 투자 조정이 가능하기 때문으로 판단된다.

Table 5. The priority analysis of investment among information security countermeasures

Higher standard	Relative investment of higher standard	Lower standard	Relative investment of lower standard	Final relative investment	Priorities
Technical/ Physical Security	0.497	System development security	0.138	0.069	6
			NO. 4		
		Cryptography control	0.133	0.066	7
			NO. 5		
		Access control	0.278	0.132	2
			NO. 1		
		Operations security	0.179	0.089	5
			NO. 3		
		Physical security	0.272	0.185	3
			NO. 2		
Prior administrative security	0.243	Information security policies	0.113	0.028	13
			NO. 6		
		Information security organization	0.142	0.034	11
			NO. 4		
		Security of External Parties	0.235	0.057	8
			NO. 1		
		Information asset classification	0.177	0.043	10
			NO. 3		
		Education and training on information security	0.134	0.032	12
			NO. 5		
		Personnel security	0.198	0.048	9
			NO. 2		
Post administrative security	0.260	Intrusion incident handling	0.447	0.116	4
			NO. 2		
		IT disaster recovery planning	0.553	0.144	1
			NO. 1		

하위기준의 상대적 투자의 우선순위를 비교해 보면, 기술적/물리적 보안 측면에서는 접근통제가 가장 투자가 많이 이루어진 것으로 나타났으며, 사전 관리적 보안에서는 외부자 보안이 가장 투자가 많이 이루어진 것으로 나타났다. 상대적 중요도와 마찬가지로 일련의 개인정보유출 사건으로 인해 주요 시스템 및 정보에 대한 접근을 관리하는 영역에 대한 투자가 많이 이루어진 것으로 판단된다. 반면에 인적보안보다 외부자 보안에 투자가 더 많이 이루어진 이유는 내부인력에 비해 신뢰성이 상대적으로 떨어지는 외부자에 대한 보안 투자가 현실적으로 더 설득력을 갖기 때문인 것으로 설명된다.

사후 관리적 보안 측면에서는 침해사고 관리보다 IT 재해복구에 대한 투자가 더 많이 이루어진 것으로 확인된다. 이러한 결과의 이유는 IT 재해복구는 백업 DB 및 방재설비 구축 등과 같이 정보시스템을 운영하는 조직에 공통적으로 적용되는 사전 대비 성격의 투자이지만, 침해사고 관리는 실제로 침해사고를 당한 조직에서 발생하는 투자이기 때문으로 판단된다.

상위기준 간의 중요도와 투자 우선순위를 비교하

Table 6. The comparison priorities between perceived importance and investment

Higher standard	Relative importance ranking of higher standard	Relative investment ranking of higher standard	Lower standard	Relative importance ranking of lower standard	Relative investment ranking of lower standard
Technical / Physical Security	2	1	System development security	8	6
			Cryptography control	13	7
			Access control	2	2
			Operations security	9	5
			Physical security	6	3
Prior administrative security	1	3	Information security policies	7	13
			Information security organization	10	11
			Security of External Parties	11	8
			Information asset classification	12	10
			Education and training on information security	5	12
			Personnel security	3	9
Post administrative security	3	2	Intrusion incident handling	1	4
			IT disaster recovery planning	4	1

였을 경우, 중요도에서는 사전 관리적 보안이 가장 순위가 높았던 반면, 투자에서는 기술적/물리적 보안의 순위가 가장 높고 사전 관리적 보안이 가장 낮았다. 이런 결과는 조직 내에 정보보호 조직과 체계를 구축하는 것보다 정보보호 시스템 및 솔루션 도입을 통한 가시적 성과 도출을 우선시하기 때문으로 판단된다. 실제로 한국인터넷진흥원[9]의 정보보호 실태조사에 따르면 국내 종사자 수 5인 이상인 사업체 중 9.8%만이 정보보호 전담조직을 운영하고 있으며, 20.%가 정보보호 정책을 수립한 것으로 나타났다.

정보보호대책 중 상대적 중요도와 투자 우선순위의 차이가 큰 항목은 암호통제, 정보보호 정책, 정보보호 교육, 인적보안으로 확인되었다.

암호통제는 정보유출 시 해당 정보를 확인할 수 없도록 하는 마지막 단계의 보안 절차이기 때문에 낮은 중요도를 갖는 반면, 개인정보관련 법률에서 개인정보 암호화를 의무화함에 따라 투자의 우선순위가 높아진 것으로 볼 수 있다.

정보보호정책은 조직 내에서 임직원이 준수해야 할 정보보호 사항들을 명시한 문서로서 조직의 특성과 상황을 정확히 분석하여 수립되어야 하는 필수적 사항이다. 하지만 표준적으로 공유되는 정보보호정책을 자사의 상황에 맞게 변경하는 것이 일반적이기 때문에 투자의 우선순위가 낮은 것으로 판단된다.

조직 내에서 정보보호 강화를 위해 가장 중요한 것 중에 하나가 조직원의 보안인식 수준을 높이는 것이다. 이를 위해 정기적인 보안 교육이 시행되어야 하며 법률에서도 정보보안담당자에 대한 정기적인 교육을 의무화하고 있다. 하지만 교육의 효과가 나타나기까지 일정 시간이 필요하기 때문에 투자 우선순위에서 밀리는 것으로 볼 수 있다.

최근의 정보유출 사건이 내부자 유출에 기인한다는 점에서 인적보안은 매우 중요하다. 하지만 상대적으로 인적보안에 대한 투자가 낮은 이유는 외부자에 비해 상대적으로 내부 직원에 대한 신뢰가 높으며, 보안준수가 일상화된 조직문화를 형성하는 데에는 많은 시간과 노력이 필요하기 때문으로 판단된다.

VI. 결론 및 시사점

본 연구의 결과를 다음과 같이 요약할 수 있다. 첫째, 정보보호 중요도 평가에서 상위기준 중 사전 관리적 보안이 가장 중요한 것으로 확인되었으며, 하위기준에서는 침해사고 관리가 가장 중요한 것으로

나타났다. 둘째, 정보보호 투자정도 평가에서 상위기준 중 기술적/물리적 보안이 투자 정도가 높은 것으로 나타났으며, 하위 기준에서는 IT 재해복구가 가장 높은 것으로 확인되었다. 셋째, 정보보호 중요도와 투자 간의 우선순위 차이가 큰 정보보호 항목은 암호통제, 정보보호 정책, 정보보호 교육, 인적보안으로 확인되었다.

연구 결과를 바탕으로 도출된 본 연구의 주요 시사점은 다음과 같다. 첫째, 조직 내 정보보호를 강화하기 위해서는 사전 관리적 보안 측면의 정보보호항목들을 우선적으로 고려해야 한다. 조직의 현 상황을 정확히 분석하여 적절한 정보보호 준수사항들을 수립하고 조직을 구성하는 것이 여기에 해당된다. 조직의 정보보호 운영과 관리의 기본적인 토대 역할을 한다는 점에서 가장 우선적으로 고려되어야 하지만, 단기적인 정보보호의 성과를 위해 간과되거나 형식적으로 시행되는 경우가 일반적이다. 그리고 가시적 성과를 위해 정보보호 시스템과 솔루션을 우선적으로 도입하는 경우가 많다. 기업들은 장기적 관점에서 전문적인 인력을 채용하고 효율적인 정보보호 관리체계를 수립하여, 조직원 모두에게 공유하고 참여를 유도하는데 노력을 기울여야 한다.

둘째, 최근의 개인정보유출 사건에서 볼 수 있듯이 보안사고가 직접적인 재무적 손실로 이어지기 때문에 적절한 대응을 통한 피해를 최소화 하는 것이 중요하다. 하지만 침해사고 관리는 사후에 그 필요성을 인지하는 경우가 많아 사전 준비에 소홀하게 되는 경우가 많다. 또한, 침해사고 관리 능력은 단기간에 형성되지 않는다. 조직원들의 반복적인 학습과 연습을 통해 긴급한 사고 상황에 대한 적절한 대응 능력을 확보할 수 있다. 따라서 기업들은 보안사고에 대한 대응 절차를 수립하고 정기적인 모의점검을 통해 대응방법에 대한 관리와 개선을 지속적으로 실행해야한다.

셋째, 정보유출 사건의 주요 원인이 내부자 유출이라는 점을 고려하여 인적보안에 중심을 둔 접근통제가 이루어져야 한다. 그동안 접근통제가 비권한 외부자에 대해 초점이 맞춰져 있었다면 앞으로는 중요한 정보자산에 접근을 하는 내부자 관리를 강화해야 한다. 사실, 내부자가 외부자에 비해 주요 시스템의 접근이 용이하다는 점에서 내부자의 접근통제에 대한 관리와 투자가 더 우선시 되어야 한다.

넷째, 정보보호정책과 정보보호교육은 중요도에 비해 투자가 상대적으로 많이 부족한 항목들이다. 정보보호정책은 정보보호 준수사항들을 세부적으로 명시하고 있기 때문에 조직원 모두에게 공유되고 법률 및 사회적 변화에 맞추어 지속적으로 갱신이 이뤄져야 한다. 그리고 정보보호정책에 대한 조직원들의 인식을 높이고 참여를 유도하는데 있어서 정보보호교육은 효과적인 방법 중에 하나이다. 따라서 기업들은 정보보호 강화를 위해 조직의 특성에 맞게 정보보호정책을 수립하고 주기적인 교육을 통해 조직원의 인식과 참여를 높이는 활동을 적극적으로 지원해야 한다.

다섯째, 무엇보다도 정보보호전문가의 중요도 인식과 실제 투자 현황에서의 차이는 정보보호관련 투자가 전문가의 의견보다 조직 내부의 정치적 영향이나 외부 규제 등의 영향에 좌우됐다는 점에서 우려를 갖게 된다. 기업 내에서 실질적인 정보보호전문가의 위상과 의사결정 권한에 대한 재고가 필요한 시점이라고 볼 수 있다.

본 연구는 다음과 같은 한계점을 가지고 있다. 첫째, ISMS 인증의 13개 정보보호대책 항목을 평가기준으로 도출하였다. 하지만 ISMS가 조직 내 정보보호에 초점이 맞춰져 있기 때문에 최근에 이슈가 되고 있는 개인정보보호를 고려하여 PIMS(Personal Information Management System) 인증의 항목까지 반영하여 연구할 필요가 있다.

둘째, 본 연구에서는 업종이나 기업 규모를 고려하지 않았다. 조직 내 정보보호관리체계를 도입하여 운영할 때, 업종이나 기업 규모에 따라 차이가 있을 수 있기 때문에 기업의 업종, 규모 등을 고려하여 좀 더 세밀하게 비교·분석할 필요가 있다.

마지막으로 향후 관련 연구에서는 13개 정보보호대책 항목에 대해 예산 소요 및 법령 의무사항 여부를 추가적으로 고려할 필요가 있다. 각 정보보호항목의 중요도 평가에서 이 두 가지 요인은 중요한 영향을 미칠 수 있기 때문이다.

본 연구는 국내 표준으로 활용되고 있는 ISMS 인증의 정보보호대책 항목을 기반으로 상대적 중요도와 투자 정도를 비교·분석함으로써 국내 기업들에게 공통적으로 적용할 수 있는 정보보호항목들에 대한 우선순위를 처음으로 제공했다는 점에서 의의가 있다. 또한 본 연구 결과는 정보보호관리체계를 도입을 고려하거나 운영 중인 기업들이 한정된 예산을 고려하여 효과적인 정보보호 투자에 대한 의사결정 자료로 활용될 수 있을 것으로 기대한다.

References

[1] Dong-yeup Lee, Tae-ho An and Yong-su Hwang, "Analysis of the priorities of the major science and technology areas in the national R&D investment by AHP method," Journal of Technology Innovation, 10(1), pp. 83-97, Jul. 2002.

[2] Jeong-woo Chae and Jin-hong Jeong, "Study on decision making for the industrial security management factor's priority," Journal of Security Engineering, 10(2), pp. 123-140, Apr. 2013.

[3] Jin-kyu Kang and Byong-chan Min, AHP Theory and Practice, INTERVISION, 2008.

[4] Ji-sook Kim, Soo-yeun Lee and Jong-in Lim, "Comparison of The ISMS Difference for Private and Public Sector," Journal of the Korea Institute of Information Security and Cryptology, 20(2), pp. 117-129, Apr. 2010.

[5] Keun-tae Cho, Yong-kon Cho and Hyun-su Kang, Analytic Hierarchy Process of ahead leaders, DongHyeon Inc, 2003.

[6] Keun-tae Cho, Seoung-joon Kim, Dae-sik Kim, Young-woo Cho and Jong-in Lee, "Priority Setting for Future Core Technologies using the AHP: With Major Fields in Rural Development and Resources," Journal of Korean Society of Rural Planning, 9(3), pp. 41-46, Aug. 2003.

[7] Ki-chul Kim and Seung-joo Kim, "Evaluation Criteria for Korean Smart Grid based on K-ISMS," Journal of the Korea Institute of Information Security and Cryptology, 22(6), pp. 1375-1391, Dec. 2012.

[8] Korea Internet & Security Agency, A handbook on ISMS certification system, Jun 2013.

[9] Korea Internet & Security Agency, 2013 Research on the actual condition of the information security, Dec. 2013.

[10] Korea Internet & Security Agency, http://imsm.kisa.or.kr

[11] Kyong-sik Kim and Min-hyuk Kwon, "The Development and Application of the Scale on the Participation Constraints of Sport for All," Korean Journal of Societegy of Sport, 20(2), pp. 159-173, Jun 2007.

[12] Subrata Biswas, Jin-ho Yoo and Chul-yong Jung, "A Study on Priorities of the Components of Big Data Information Security Service by AHP," Journal of Society for e-Business Studies, 18(4), pp. 301-314, Nov. 2013.

[13] T. L. Saaty, The Analytic Hierarchy Process, McGraw-Hill Inc, 1980.

[14] T. L. Saaty, "Priority Setting in Complex Problem," IEEE Transaction on Engineering Management, 30(3), pp. 140-155, Aug. 1983.

[15] T. L. Saaty, Decision-Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World, RWS Publications, 1995.

[16] Tae-sung Kim and Hyo-jung Jun, "Analysis on Information Security Manpower Policy by the Analytic Hierarchy Process," Journal of the Korea Institute of Information Security and Cryptology, 31(5B), pp. 486-493, May 2006.

[17] Young-sik Bae, "A study Effect of Information Security Management System[ISMS] Certification on Organization Performance," Journal of the Korea Academia-Industrial, 13(9), pp. 4224-4233, Sep. 2012.

〈저자소개〉

이 중 정 (Choong-Cheang Lee) 정회원
1982년 2월: 연세대학교 교육학사 졸업
1986년 2월: University of Rhode Island 경영학 석사 졸업
1993년 2월: University of South Carolina MIS 박사 졸업
1991년 3월~1993년 8월: Univ.of South Carolina, Dept. of Information & Decision Sciences, 연구원
1993년 9월~2001년 8월: Salisbury State University, 부교수
2001년 9월~현재: 연세대학교 정보대학원, 교수
〈관심분야〉 IT performance, IT evaluation measurement, Information Orientation

김 진 (Jin Kim) 정회원
2000년 2월: 홍익대학교 금속재료공학과 졸업
2014년 2월: 연세대학교 정보시스템학 정보미디어전략 석사
2008년 1월~현재: 삼정KPMG 차장
〈관심분야〉 정보보호, IT ROI, 정보시스템감리, IT 아웃소싱

이 충 훈 (Chung-Hun Lee) 정회원
2005년 2월: 건국대학교 경제학과 졸업
2013년 2월: 연세대학교 정보대학원 지식서비스보안 석사 졸업
2013년 3월~현재: 연세대학교 정보대학원 IT서비스 전략기획 및 관리 박사과정
〈관심분야〉 정보보호, 프라이버시, IT service, IT performance, 디지털 비즈니스