http://dx.doi.org/10.15207/JKCS.2015.6.4.033

산업융합환경을 위한 보안 거버넌스 프레임워크 설계

이효직[1*], 나원철[1*], 성소영[1*], 장항배[2]
[1]중앙대학교 융합보안학과, [2]중앙대학교 산업보안학과

A Design on Security Governance Framework for Industry Convergence Environment

Hyojik Lee[1*], Onechul Na[1*], Soyoung Sung[1*], Hangbae Chang[2]
[1]Department of Security Convergence, ChungAng University
[2]Department of Industriatl Security, ChungAng University

요 약 산업과 ICT 기술간의 융합으로 새로운 부가가치를 창출할 수 있는 융합환경이 도래되어짐에 따라 경제성장과 더불어 우리의 삶의 질이 향상 되고 있지만 이러한 융합환경은 다수의 이익만을 제공하는 것이 아니라 융복합적인 보안 위협이 발생됨에 따라 다양한 보안문제를 발생시켰다. 이러한 보안 문제를 해결하기 위해서는 기존의 기술적인 접근으로 단편적인 보안 문제 해결방식이 아닌 통합적인 관점에서 보안문제를 접근할 필요가 있다. 그래서 본 연구에서는 전략적 관점, 관리적/운영적관점, 기술적 관점 등 다차원적인 관점에서 신뢰성 있는 보안 거버넌스 관리를 할 수 있도록 인적측면이 고려되어진 보안 거버넌스 프레임워크를 개발하였다. 그래서 이 프레임워크를 통해 보안 관리에 대한 단일 기준을 제시함으로서 최고 경영진들의 직접적인 관여가 가능하고 조직구성원들이 스스로 보안활동을 수행하고 책임 질수 있는 신뢰성 있는 보안관리체계를 구축할 수 있을 것이다.

• Key Words : 융합환경, 보안 거버넌스, 보안문화, 보안윤리, 정보보호관리체계

Abstract According to arriving convergence environment which can create new value-added converged between industry and ICT technology, It has made economic growth and improve the quality of life. However this convergence environment provide not only advantage but also various security problems resulting from generating converged security threats. For resolving this security problem, we need to approach to security problem in the integrated view not the fragmentary view which cover only technical approach. So This study developed security governance framework which can manage trustful security governance in multidimensional view which cover strategy, managerial/ operational and technical view. Therefore this framework can construct trustful security management system which can help top management team to engage in security management directly and organizational member to perform security activities and have responsibility for themselves as suggesting single standard for security management.

• Key Words : Convergence Environment, Security Governance, Security Culture, Security Ethics, Information Security Management System

*교신저자 : 장항배(hbchang@cau.ac.kr)
접수일 2015년 5월 11일 수정일 2015년 7월 21일 게재확정일 2015년 8월 20일

1. 서론

산업 환경은 각자의 전통적인 가치사슬을 벗어나 새로운 부가가치의 창출을 위해 산업 간, 기술 간의 융합화가 가속화되어 지능형, 고부가가치형을 추구하는 융합 환경으로 변화하고 있다. 이러한 융합 환경이 도래함에 따라 새로운 부가가치를 창출하고 경제성장과 더불어 삶의 질이 향상되었다. 하지만 이러한 융합환경으로 변화는 장점만을 제공해주는 것이 아니라 기존 전통전적인 보안의 범위를 포함하여 사기, 물리적 절도, 사회 공학 기법, 상표 침해, 산업 스파이 핵심 인력 매수, 데이터 위·변조 등 융 복합적 보안 문제를 발생시켰다. 이와 같은 융 복합적인 보안 문제를 예방하기 위해서는 기존보안 환경에서 치중했던 기술적인 관점만의 단편적인 접근으로 보안 문제를 다루어서는 안 된다. 융 복합적인 보안 위협이 존재하는 융합 환경에서 효과적인 보안을 수행하기 위해서 관리적, 기술적, 물리적, 인적 등 다차원적인 관점으로 보안 문제를 접근해야 한다. 그리고 최고 경영진으로부터 전체 조직 구성원까지 전사적으로 보안활동을 수행하고 책임 질수 있는 보안 문화를 창출 할 수 있고 기술적·절차적 체계뿐만 아니라 인간행동까지 함께 고려한 보안 거버넌스 체계에 대한 필요성이 존재한다. 그래서 본 연구에서는 적정 수준의 보안 문화를 구축하기 위해 경영진이 보안 계획에서부터 조직 구성원의 행동 관련 규범을 만들어 갈 수 있도록 하고 이를 통해 조직 구성원이 직접 보안활동을 수행하고 책임 질 수 있게 하는 보안 거버넌스 프레임워크를 만들려고 한다. 그리고 과거의 기술적·절차적 체계뿐만 아니라 전략적, 인적 요소등이 포함된 융 복합적인 체계를 갖춘 보안 거버넌스 프레임워크를 개발하려고 한다.

2. 관련 연구

2.1 보안 거버넌스의 정의

NIST에서 SP 800-100에 의하면 , 정보보호 거버넌스는 “위험관리 노력의 한 부분으로서, 정보보호 전략이 비즈니스 목표와 연계되어 이의 달성을 지원하며, 정책과 내부통제 등을 통해 관련 규정과 법규를 준수하는 것을 보장하고 책임을 할당하기 위한 프레임워크와 이를 경영구조 및 프로세스를 수립하는 과정”으로 정의하고 있다[1,2]. 일단 정보보안 거버넌스는 정보자산의 보호, 서비스 연속성, 정보의 무결성이라는 3가지 목적으로 시작된다[3]. 정보보안 거버넌스는 기업 거버넌스의 부분집합으로서 전략적 방향을 제시하며, 목적 달성, 조직자산의 책임 있는 사용, 적절한 위험관리, 기업보안프로그램의 성공과 실패가 모니터링 됨을 보장한다[4]. 정보보안 거버넌스는 조직의 목적을 지원하기 위한 최적화된 정보보안 투자, 정보보안과 사업전략 연계, 정보보안 지식과 인프라스트럭처를 효과적이고 효율적으로 이용, 잠재적 영향을 용인 가능한 레벨로 감소시키기 위한 적절한 측정, 정보자산에 대한 위험 관리/완화, 모니터링과 보고 외에도 프로세스 통합, 보증이라는 부분을 가진다. [5]. 이와 같이 정보보안 거버넌스는 기업의 한 부분이며, IT 거버넌스와도 종속적인 아닌 상호 보완적적인 맥락으로 구분된다[6]. 정보보안이 포화상태에 치닫고 있는 현시점에서, 여전히 기업기밀 유출사고는 보이지 않는 곳에서 일어나고 있다. 이는 정보보안 거버넌스를 통해 전사적 차원의 관리가 시급하다는 것으로 기업이 측정하는 보안 비용에 비해 위험 비용이 월등히 높아 아직도 기업의 경영진들은 정보보안사고에 대해 소극적으로 대처하고 있다. 이에 정보보안 거버넌스 프레임워크를 통해 대기업이 아닌 보안 비용을 많이 투자를 할 수 없는 수많은 중소기업의 정보보안에 기여할 수 있고 이는 중소기업의 시장경쟁력 강화에 기여하게 된다. 여기서 보안 거버넌스는 산업보안 위험관리체계를 기초로 하여 조직의 가치를 상승시키기 위한 조직 구성요소들의 협력체계로서 조직 구성요소 체계의 유기적인 협력을 위해서는 조직 구성원들의 소속감이나 위상이 제고되어 명확한 성과 관리체계가 수립되어야 한다. 타 부서와의 협업 매커니즘 수립과 컴플라이언스 관리체계 수립 또한 중요하다. 특히, 지속적인 컴플라이언스 모니터링 및 준거성확보는 산업보안 위험관리체계와 거버넌스 체계 확립에 기반이 될 수 있다[7].

2.2 보안거버넌스 프레임워크에 대한 선행 연구

2.2.1 ISO /IEC 177995 and ISO /IEC 27001

ISO/IEC 177995는 위험도 평가 및 대응방안 마련을 위한 방법론으로 과거 미국 및 유럽 등 세계 각국에서 만들어 왔던 방법론들을 국제표준으로 통합한 것이다[8]. 이 표준 방법론에서 정보 자산의 가치는 조직에 미치는 영향력을 기본으로 측정하는데 자산의 특성에 맞게 정성적 또는 정량적인 방법으로 가치를 평가 할 수 있다. 정보보호를 위해 필수적인 기준으로 인식되어 지고 있는

ISO/IEC 177995는 11개 통제항목 세션으로 이루어지고 있다. ISO 27001은 “정보보안관리 실무 규범“이라는 제목 하에 조직의 정보보호를 구현하고 유지하는 보안 관리자들이 참조할 수 있는 가이드라인으로 사용하도록 개발되었다. ISO27001는 11개의 관리영역 분야, 39개의 통제목표 분야, 그리고 133개의 통제항목으로 구성되어 있으며, 현재 사용하고 있는 보안 표준 중 가장 실무적인 정보보안 통제항목을 제공하고 있다[9].

2.2.2 PROTECT

Eloff and Eloff(2005)는 PROTECT라는 포괄적인 관점으로 정보보안을 접근하는 프레임워크를 개발하였다. PROTECT는 위험 감소 및 조직 경영의 효율성을 보장하기 위해 정보보호의 정책, 리스크, 목표, 기술 등의 다양하고 융합적인 통제요소를 다루었다. 7가지의 통제요소로 이루어진 PROTECT는 기술적인 측면뿐만 아니라 인간적인 측면을 다룸으로서 효과적인 보안 프로그램 수행 및 관리에 초점을 맞추고 있다[10]. 그리고 이 접근법은 유일하게 윤리적 가치를 언급하였다. 이 접근법은 매우 포괄적이기는 하나 업무 연속성이나 사고 관리 등의 측면이 정책 및 프로세스 요소에서 다루어질 수 있지만 명시하고 있지 않다[11].

2.2.3 Capability Maturity Model

McCarthy and Campbell(2001)가 Security Transformation에서 제시한 Capability Maturity Model은 정보 자산에 대한 비인가적인 접근, 수정, 파괴로부터 보호 할 수 있는 보안 통제 구성 요소를 제공하고 있다. 통합적인 관점에서 정보 보안을 다루고 있는 이 모델은 7가지 주요 보안 통제 요소를 다루고 있다. 이 모델은 정보보안이 전략적 단계에서 시작되어 전략적 단계에서 제시한 방향성을 반영한 기술적 단계까지 이어져야함을 설명한다[12].

2.2.4 Information Security Architecture(ISA)

Tudor(2000)가 제시한 Information Security Architecture은 보안위협으로부터 조직의 자산을 보호하기 위해 포괄적이고 융통성 있는 정보보안 아키텍처를 제공하였다. 이 아키텍처는 보안 위험을 감소하기 위한 보안 통제 사항을 수행하고 평가하기 위해 조직의 위험 환경을 이해 할 수 있는 5가지 주요 보안 원칙을 강조하였다. 특히 Tudor의 접근법에서는 보안 요소로서 유일하게 신뢰를 언급하였다. 이 아키텍처의 보안 요소 중 기업 운영, 윤리적 숙고와 신뢰는 사회공학, 사기 및 직원의 정보 시스템 오용 등의 리스크들을 처리할 수 있는 포괄적 보안 구성요소들을 제공하기 위해 조직이 차용하는 접근법에 포함될 필요가 있다고 설명하였다[13].

2.3.5 Information Security Culture Framework (ISCF)

Da Veiga(2010)는 조직에 정보보호 문화를 측정하기 위한 산정 수단으로서 Information Security Culture Framework(ICSF)를 개발하였다. Information Security Culture Framework는 정보보안문화를 효과적으로 형성하기 위해 전략적 계획부터 조직구성원의 행동가이드의 통제항목을 포괄적으로 제공함으로서 조직구성원의 행위적인 관점에서 보안 프로그램 수행 및 관리를 하는데 초점을 맞추고 있다. 7개 주요 정보보호 통제요소를 다루고 있고 각 통제요소를 정보보호 행동에 영향을 미칠 수 있는 조직, 그룹, 개인 등 총 3개 계층 별로 구분하여 배치하였다. Da Veiga는 효과적인 보안 문화를 형성 하기 위해서는 각 계층별에 이루어진 통제항목은 서로 연관되어 영향을 미칠 수 있기 때문에 조직에서부터 개인의 계층까지 모든 계층에서 효과적인 보안 통제 및 활동이 이루어져야 한다고 설명하고 있다[14].

2.3.6 K-ISMS

K-ISMS는 국내 정보보호 관리체계 인증제도로서 국제 표준인 ISO 27001을 기반으로 국내 실정에 맞게 정보보호 관리과정을 5단 사이클과 1개 통제항목으로 관리한다. 그리고 정보보호 대책과 관련된 15개 분야의 120개 통제항목과 문서화와 관련된 3개 통제항목을 합한 총 137개 통제항목과 446개의 세부적인 통제항목을 적용한 국내 정보보호 관리체계로 관리과정을 위험 분석기반으로 단계별 구축하게 하여 조직에 규모와 형태, 종류와 관계없이 국내표준모델로서 적용이 가능하다는 점이 특징이다. 그리고 정보보호 조직으로부터 업무 연속성 관리까지 ISO 국제표준을 모두 포함하고 있으며 국내 실정에 맞게 전자거래, 암호화, 침해사고 예방 등의 보안 요건을 강화하였다[15].

3. 보안 거버넌스 프레임워크 구성 요소 도출

우선적으로 보안 거버넌스 프레임워크를 개발하기 위해 보안 거버넌스 프레임워크 안에 구성할 요소들을 도출하려고 한다. 보안 거버넌스 프레임워크의 구성요소를 도출하기 위해 기존 선행연구를 참고하였으며 1)ISO 17799의 관련 섹션, 2) PRTECT 구성요소들, 3) 조직성숙도 평가 모델의 단계들과 4) ISA접근법의 원칙의 보안 구성요소 5) ISCF의 보안구성요소 6) K-ISMS의 관련 통제항목 등 구성요소를 매핑을 하여 각 접근법에 따르는 구성요소의 범위 및 구성요소 포함 비율를 나타냈다. 기존 선행연구를 매핑 분석한 결과는 아래의 <Table 1>과 같다.

〈Table 1〉 Information Security Governance Approach Component

Security Components	1)	2)	3)	4)	5)	6)
1 Corporate governance	X	X	X	X	●	X
2 Information security strategy	X	X	●	X	X	X
3 Leadership in Terms of Guidance and Executive Level representation	●	●	●	●	●	●
4 Security organization (Internal Organization such as Management Commitment, Responsibility, and Coordination; External Parties)	●	●	●	●	●	●
5 Security Policies, Standard, and guidelines	●	●	●	●	●	●
6 Measurement / Metric / Return on Investment	X	●	●	X	●	X
7 Compliance and Monitoring (Legal, Regulatory, and Auditing))	●	●	●	●	●	●
8 User Management(User, Joiner, and Leaver Process)	●	X	●	X	●	●
9 User awareness, Training, and Education	●	●	●	●	●	●
10 Ethical Values and Conduct	X	●	X	X	●	X
11 Privacy	X	X	●	X	X	X
12 Trust	X	X	X	●	●	X
13 Certification against a standard	●	●	X	X	●	●
14 Best Practice and Baseline Consideration	●	●	●	●	●	●
15 Asset management (Responsibility and Classification)	●	●	X	●	●	●
16 Phisical and EnvironmentalControls(Secure areas and equipment	●	●	●	●	●	●
17 Technical Operation(e.g., Anti-Virus, Capacity, Change Management, and System Development)	●	●	●	●	●	●
18 System Acquisition, Development, and Maintenance	●	●	●	X	●	●
19 Incident Management	●	X	●	X	●	●
20 Business Continuity Planning(BCP)	●	X	●	●	●	●
21 Disaster Recovery Planning(DRP)	X	X	●	●	X	●
22 Risk assessment Process	●	●	●	●	●	●
Number of Components derived from each approach	15	14	17	13	19	16
Percentage	68 %	63 %	77 %	59 %	86 %	72 %

각 선행연구의 구성요소들을 매핑한 결과 ISO/IEC 17799, McCarthy and Campbell의 조직 성숙도 평가 모델 구성요소, Da Veiga의 ISCF 보안요소 와 K-ISMS통제항목은 보안 구성요소들의 범위를 다루는데 있어 포괄적이기 때문에 Eloff and Eloff와 Tudor의 접근법과 비교해 보았을 때 포함 비율이 높은 것으로 나타난다. 그리고 Eloff and Eloff (2005)의 접근법은 유일하게 윤리적 가치를 구체적으로 언급하였고 Tudor (2000)의 접근법에서는 유일하게 신뢰를 언급했듯이 여러 연구자들은 보안 거버넌스를 위하여 다양한 관점에서 보안요소를 다루고 있음을 알 수 있었다.

그래서 본 연구에서는 보안 거버넌스 선행연구 매핑 분석의 결과를 통해 선행연구의 각 구성요소들이 3개 이상 겹치는 경우 보안 구성요소로서 중요도가 높다고 판단하여 보안 거버넌스 구성요소 목록으로 도출하였다. 하지만 나머지 구성요소 경우 선행연구에서 보안구성 요소로서 많이 다루지는 않았지만 전문가 회의를 통해서 탈락 당위성에 대해 다시 한번 회의를 하였고 그중에 가장 핵심적으로 현대사회에서 반드시 지켜야 할 보안윤리를 보안거버넌스를 갖추기위해 필요한 보안요소라고 판단하여 보안구성요소 목록으로 도출하였다. 그 외에 기업 운영, 신뢰와 프라이버시와 같은 보안 요소는 여러 연구자들이 보안 거버넌스를 위하여 포함 여부를 고려하였음에도 불구하고 다른 보안 요소와 내용적인 면에서 겹치는 부분이 많이 있다고 판단하여 조직 내 보안 거버넌스를 구축하기 위한 요소 도출 시 포함하지 않고 다른 요

소에 다룰 수 있도록 통합을 하였다. 이와 같은 결과를 통해 도출한 보안 거버넌스 프레임워크의 세부 구성요소는 보안투자, 리스크 평가, 보안계획, 보안성과분석, 보안조직 및 보안역량, 보안정책 및 규정/ 프로세스, 보안의식, 보안교육, 보안 윤리, 신뢰, 공통(법) 준수사항(준거성), 보안감사, 공통자산현황 관리 / 업종특화 자산현황 관리 / 자산분류/등급, 시스템 개발/운영/유지보수(용역관리포함), 물리적 영역(공간)보안 / 물리적 장비보안 / 공통정보시스템 보안/업종특화 정보시스템 보안, 업무연속성, 사고대응체계, 재난복구계획 등 총 18개의 세부 보안요소로 구성하였다.

4. 보안 거버넌스 프레임워크 개발

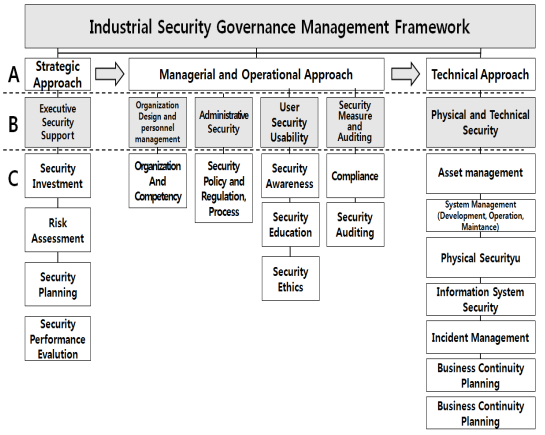
위 보안 거버넌스 프레임워크 구성요소 개발을 통해 도출한 세부 구성요소를 토대로 보안 거버넌스 프레임워크를 개발하였다.

일단 보안 거버넌스 프레임워크를 개발하기 위해 보안 거버넌스 체계를 A,B,C의 총 3단계로 분할하였다. 첫 번째로 A 단계는 전략적, 관리적 / 운영적 그리고 기술적 관점 등 3가지 관점으로 보안 거버넌스 체계를 구분하였다. 두 번째로 B 단계는 3가지 A 단계에서 구분했던 3가지 관점에 따라 6가지 주요 보안 요소를 배치하여 구성하였다. 6가지 주요 보안 구성요소 목록은 아래의 <Table 2>와 같다.

〈Table 2〉 Core Security Components of Security Governance Framework

Type(A)	Core Security Components(B)
Strategic Approach	Executive Security Support (Security Responsibility)
Managerial and Operational Approach	Organization Design and personnel management
	Administrative Security
	Security Measure and Auditing
	User Security Usability
Technical Approach	Physical and Technical Security

마지막으로 C단계에서는 B단계의 6가지 주요 보안 구성 분류에 맞춰 기존 선행연구 분석을 토대로 추출한 보안 거버넌스 세부 구성요소를 배치시켰다. 위 과정을 통해 개발한 보안 거버넌스 프레임워크는 아래의 그림 [Fig. 1] 과 같다.



[Fig. 1] Security Governance Framework

앞서 말한 바와 같이 보안 거버넌스 프레임워크에서는 3가지 접근방법에서 보안관리가 이루어지고 있다. 첫 번째는 전략적 관점으로서 경영진의 보안지원(보안책임성)으로 주요 보안요소가 구성 되어있다. 경영진의 보안지원의 세부구성요소는 보안에 대한 임원진들의 보안투자와 정확한 정보보안 시행을 위해 선행되어져야하는 리스크 평가, 정보자산 보호를 위한 경영진의 보안계획 및 보안 관심정도, 그리고 보안활동 성과분석으로 구성되어 있다. 보안 거버넌스가 보고체계, 권한, 소유권, 감독 및 정책 시행 등의 조직규제를 뜻하는 기업 거버넌스의 구성요소로 받아들여지기 때문에 보안 거버넌스 또한 조직을 건전한 리더십 노력을 통해 효과적으로 지시 및 관리해야하는 경영진의 책임과 연관이 있다. 그리고 이는 조직이 조직 내 기술 사용과 핵심 기술 보호를 지시 및 관리하는 방법을 정의하는 정책과 절차에 관한 IT 거버넌스와도 관련이 있다. 그렇기 때문에 경영진 보안지원(보안 책임성)의 세부 구성요소는 위험 경감 전략과 필수 규제 파악에 목적을 둔 보안 활동을 실행하며 위협을 다루는 보안 계획을 포함해야하며 보안 계획은 조직의 목적이 장기와 단기적으로 이루어지게 하기 위해 조직적 IT 전략과 연동되어야한다. 그리고 경영진 보안지원(보안책임성)의 세부 구성요로서 효과적인 조직이 보안 위협을 다루는 방법을 측정하기 위한 보안활동 성과분석이 포함되어야하는데 보안 사고의 수 혹은 인식의 실증적 결과들을 통해서 보안활동의 성과분석으로 사용되어 질

수 있고 이와 같은 성과분석을 통해 조직의 현재 보안 위협이 내일의 업무의 기회로서 전환하는 것을 지원할 수도 있다. 다음은 관리적/운영적 관점으로서 B단계의 주요 보안 요소는 조직설계 및 인력관리, 사용자 보안 수용성, 관리적보안(지침), 보안진단 및 감사 등이 있다. 관리적/운영적 요소의 첫 번째 주요 보안 요소인 조직 설계 및 인력관리는 보안 조직 및 보안인력 역량의 세부구성요소로 이루어져 있다. 보안 조직의 경우 기업 보안 아키텍처에 필요한 역할과 책임, 기술과 경험, 그리고 자원 수준에 따른 보안 조직 설계 및 구성원간의 보고 체계를 설립한다. 다음 구성요소로서 관리적 보안(지침)은 보안정책 및 규정, 업무처리 절차등 주요 보안 요소로 구성되어 있다. 위 구성요소는 보안 정책, 절차, 표준과 같은 보안 활동에 대한 가이드라인으로서 경영진에게 기업의 목표와 기업의 보안에 대한 지원을 나타낼 수 있는 보안 시행의 중요한 열쇠와 같다. 그래서 경영진이 직원들에게 기대하는 것이 무엇이며 그들의 보안활동에 대한 가이드라인이 무엇인지 명확하게 제시해야한다. 그렇기 때문에 경영진이 정식으로 표출하는 보안에 대한 전체적 의지와 지시를 나타내는 보안정책은 효과적인 보안을 고려한 업무처리 절차와 준수 여부를 감시를 통해 조직 내에서 시행되어져야 한다. 그리고 이와 같은 보안 정책들은 사용자 등록 및 탈퇴 등의 보안 절차 혹은 방화벽 설정 방법 등의 패스워드 표준 및 가이드라인 등의 보안 표준 등으로도 설명이 되어 질 수 있다. 다음 주요 보안요소로서 사용자 보안수용성은 보안의식과 보안교육, 보안윤리 등 세부 구성요소로 구성되어 있다. 보안 문화 창출의 원칙 중 하나인 경영진의 기업 행동강령을 개발하는 등의 윤리적 행위를 통해 기업 활동에 있어 옳은 것과 잘못된 행동을 분리 시켜 윤리적 가치와 규범을 정의함으로서 직원들이 따라야하고 조직이 시행해야 하는 행위의 윤리적 표준을 세워야 한다. 이러한 경영진의 윤리적 책임은 보안 거버넌스의 체계의 일부로서 윤리적 행위는 악의적인 기술정보 유출, 프라이버시 침해, 고객정보 판매 및 무허가 데이터 변경 등의 내부자에 의한 보안 위협의 경감을 위해 반드시 조직에 의해 관리 되어져야 하고 이러한 규율들이 보안인식 프로그램의 일환으로서 조직원들에게 배포되어져야 한다. 다음은 보안진단 및 감사로서 공통(법) 준수사항 및 보안감사의 세부구성요소로 구성되어 있다. 공통(법) 준수사항에서는 보안 준거성 확보를 위해 각 산업에 관련 있는 국가적 혹은 국제적 법규의 일부 내용 및 정보통신망법, 개인정보보호법, 전자금융거래법 등 관련 보안관련 법 규제 사항을 조직에 맞게 규정하고 조직 구성원들에게 제시한다. 기업 내 법 준수사항 측정 및 감사 시행은 필수적이며 정보시스템 사용 및 직원 행동에 모두 보안 정책 준수여부를 확인하고 감지된 사고로부터 효과적이고 적시에 응답하기 위해 감시되어져야한다. 그리고 이러한 법 준수사항과 감사는 보안 정책과 절차등이 조직의 목표와 비전과 일치하는지의 여부를 확인하는데 필수적이다. 마지막 주요 보안요소로서 기술적 요소는 물리 및 기술적 보안으로 구성되어 있다. 물리 및 기술적 보안의 세부 기술요소로서는 공통 자산현황관리, 업종특화 자산현황관리(자산식별), 자산 분류/등급 , 시스템 개발/운영/유지보수(용역관리 포함), 물리적영역 / 물리적 장비 보안, 공통 정보시스템 보안, 업종특화 정보시스템 및 제조시스템 보안, 사고 대응체계, 업무연속성 계획, 재난복구계획 등의 세부구성요소로 이루어져 있다. 기존의 전통적 보안과 관련 있는 물리 및 기술적 보안 요소는 IT 환경 확보를 위해 시행되는 기술적이고 물리적인 매커니즘을 포함한다. 반드시 보안 거버넌스 체계를 시행하기 위해서는 조직의 환경에 적합한 기술 규제와 위험들을 파악해야 하며 여기에는 자산관리, 시스템 개발 요건, 사고 관리, 네트워크 보안 등의 기술적 운영, 물리적, 환경적 그리고 재난복구 계획 등이 포함되어져야 한다. 그리고 기술 환경이 지속적으로 감시되어야 하며 시장에서의 기술 변경에 따른 위험 또한 필수적으로 다루어져야한다.

이렇게 전략적 관점, 관리적/운영적 관점/ 기술적 관점 등 다차원적인 관점에서 보안 거버넌스 관리를 할 수 있는 보안 거버넌스 관리 프레임워크를 개발함으로서 조직 내 보안 의사 결정에 변화를 가져오며 직원들의 업무 실행 방법에 영향을 미칠 수 있고 정보 보호 활동에 대한 지원 및 관리, 정보 보호 관리자와 업무관리자 사이에 관계 및 사고대응 역량을 향상 할 수 있다. 그리고 보안 거버넌스 프레임워크를 통해서 기존의 정보보안에서 치중된 외부 사이버공격뿐만 아니라 최근에 많이 발생되는 기술정보 유출, 사기 및 직원의 정보시스템 오용 등의 사회 공학적 침해기법 등 조직으로부터 발생할 수 있는 다양한 보안위협을 다루기 위한 가이드라인을 개발하고 규제를 시행하며 보안예방의 시발점으로 이용할 수 있다. 과거에 기술적인 관점으로만 보안 문제를 접근했던 문제점을 해결하고 조직들이 과거에는 간과되었던 다른 관점

의 보안 구성요소들을 살펴봄으로서 조직 내 다양한 보안위협으로부터 예방을 할 수 있게 된다. 그리고 이 보안 거버넌스 관리 프레임워크는 경영진에게 기술적, 절차적 그리고 인간적 요소들을 다루는 효과적이고 포괄적인 보안 거버넌스 프로그램을 시행할 수단을 제공하며, 4가지 논의된 접근법들과 신뢰 등 고려되지 않은 요소들을 통합시킴으로서 적정 보안 문화 수준을 가지기 위해 보안 관리에 대한 단일 기준을 제시하였다. 게다가 이와 같은 거버넌스 관리를 통해 경영진들의 직접적인 관여로 기업 보안에 대해 더 많은 주의를 기울이게 되어 조직 구성원들이 보안을 하나의 생활양식으로 생각하여 조직 내 효과적 보안 문화를 형성하기 위해 각자가 행하는 일일 업무의 하나로 편입시키고 보안 태도와 인식을 제고할 수 있다. 이러한 보안 거버넌스 프레임워크를 통해 정보자산 보호 및 기술 유출 방지를 효과적으로 시행함으로서 정부차원의 보안 사업의 투자 타당성을 제시하고 보안 정책 및 지원 사업에 대한 효율적인 관리가 가능하게 하였다. 그리고 융합환경에서 신 성장 동력 산업(원자력, 자동차, 화학 등)에 대한 안전한 해외수출을 보장할 수 있는 기초적인 토대 구축을 할 수 있게 되어 다른 국가에 비해 상대적으로 앞서있는 산업기술에 대한 보호기술의 확산을 통하여 세계시장을 주도할 수 있으며, 국내 기업의 경쟁력 강화 및 정보화 강국으로의 국가 이미지를 상승 시킬 것이다.

5. 결론 및 향후 연구

새로운 부가가치 창출을 위해 현재 산업이 융합환경으로 변화함에 따라 보안 위협 또한 융 복합적으로 광범위해졌다. 이러한 융 복합적인 보안위협을 예방하기 위해서는 기존의 기술적인 접근으로 단편적인 보안 대책을 내려서는 안되고 통합적인 관점에서 보안 문제를 접근해야한다. 그래서 본 연구에서는 전략적 요소, 관리적/운영적 요소/ 기술적 요소등 다차원적인 관점에서 신뢰성 있는 보안 거버넌스 관리를 할 수 있게 인적측면이 고려되어진 보안 거버넌스 프레임워크를 개발하였다. 본 연구에서 개발한 보안 거버넌스 관리 프레임워크는 6개의 주요 보안 요소와 16개 보안 세부보안요소로 구성 되었다. 세부보안요소의 경우 기존의 보안 거버넌스 선행연구들의 보안 구성요소를 매핑 분석을 통해 구성요소의 중요도를 고려하여 산업보안관리에서 필요한 구성요소들을 추출하였다.

본 연구에서 개발한 보안 거버넌스 관리 프레임워크는 기업이 경영전략 및 정보화전략 등과 연계한 보안 거버넌스 관리 체계를 수립할 수 있게 되어 좀 더 효율적인 보안관리체계를 구축 할 수 있을 것이다. 그리고 본 연구를 통해 적정 보안 문화 수준을 가지기 위해 보안 관리에 대한 단일 기준을 제시함으로서 최고 경영진들의 직접적인 관여가 가능해 조직 구성원들에게 효과적으로 보안문화 형성을 유도할 수 있게 하였다. 이와 같은 보안문화 형성을 통해 조직 구성원들의 보안 태도와 인식이 제고되어 조직 구성원 의해 발생할 수 있는 기업 자산보호 및 기술 유출을 좀 더 효과적으로 예방 할 수 있게 될 것이다. 향후 연구에서는 보안 거버넌스 관리 프레임워크를 토대로 산업별 비즈니스 특성과 산업기술보호 요구사항을 반영한 산업보안 수준평가 모형을 개발하려고 한다.

ACKNOWLEDGMENTS

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2015-H8501-15-1018)

REFERENCES

[1] S. I. Lee, “A Research on Information Security Governance Framework,” M.A D. Dissertation DongKuk University, 2011.

[2] SP 800-100 Information Security Handbook : A guide for Managers 2007.

[3] Information Security Governance : Guidance for Information Security Managers(www.isaca.org) 2005.

[4]Korea Microsoftware, "The Understanding of Informataion Security Technology and Management Information Security Governance", Vol. 2, 2010

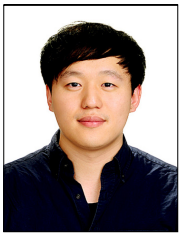
[5] M. J Kim, K. N Kim, “ A Research on Information Security Governance Framework”, Vol. 10, No. 4, pp. 13-19, 2010.

[6] W. K. Jung, “A Study on Information Security Governance Maturity Model and its Effectiveness," M.A. D. Dissertation ChungAng University, 2011.

[7] Mishra, S and Dhillon, G., "Information Systems Security Governance research : A behavioral perspective," Academic Track of 9th Annual NYS Cyber Security Conference, New York, 2007.
[8] ISO/IEC 17799 (BS7799-1) 2005.
[9] ISO/IEC 27001 (BS7799-2) 2005.
[10] Eloff, J.H.P & Eloff, M. " Integrated Information Security Architecture, Vol. 11 No. 1 pp. 10-16 2005.
[11] Da Veiga & J.H.P. Eloff, "An Information Seucurity Governance Framework", Vol. 24, pp. 361-372. 2007
[12] McCarthy, M. P. & Campbell, S. "Security Transformation", NY:MacGraw-Hill, 2001.
[13] Tudor, J. K., "Information Security Architecture-An integrated approach to security in an organization", FL: Auerbach, 2000.
[14] Da Veiga & J.H.P. Eloff, "A Framework and Assessment instrument for Information Security Culture", Vol. 29, No. 2, pp. 196-207, 2010
[15] Kisa Information Security Management System(K-ISMS) 2002.

저자소개

이 효 직(Hyo-Iik Lee) [학생회원]



- 2015년 2월 : 숭실대학교 글로벌 통상학과 졸업(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과 석·박사 통합과정

<관심분야> : 정보보호, 산업보안, 보안문화, 클라우드보안

나 원 철(One-Chul Na) [학생회원]

- 2014년 8월 : 한성대학교 컴퓨터공학과 졸업(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과 석사과정

<관심분야> : 정보보호, 융합보안, 개인정보보호

성 소 영(So-young Sung) [학생회원]

- 2013년 8월 : 상명대학교 경영학과 졸업(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과 석사과정

<관심분야> : 산업보안, IT협업, 개인정보보호

장 항 배(Hang-Bae Chang) [정회원]

- 2006년 2월 : 연세대학교 정보시스템관리 전공(박사)
- 2007년 3월 ~ 2012년 2월 : 대진대학교 경영학과 조교수
- 2012년 3월 ~ 2014년 2월 : 상명대학교 경영학과 조교수
- 2014년 3월 ~ 현재 : 중앙대학교 산업보안학과 부교수

<관심분야> : 중소기업 정보보호, 정보 오남용 및 유출 방지, 성과분석 체계