Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.3, Jun. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.3.617

기업의 상시 보안관리 체계 연구

노 시 영,[1†] 임 종 인[2‡]
[1]삼성SDS, [2]고려대학교 정보보호대학원

A Study for Enterprise Type Realtime Information Security Management System

Shi-Yeong Noh,[1†] Jong-in Lim[2‡]
[1]SamsungSDS, [2]Graduate School of Information Security, Korea University

요 약

많은 기업에서 핵심 정보자산의 보호를 위해 보안관리 체계 강화 목적으로 ISO27001, 또는 K-ISMS 등 표준 보안관리 체계를 도입하여 일정부분 성과를 얻고 있으나 최근 IT 기술의 발전과 침해수법의 진화 등으로 위협요인이 기하급수적으로 증가하고 있어 기업은 보안관리 측면에서 보다 더 신속하고, 정확한 대응조치가 필요하게 되었다. 이를 위해 보안관리 프로세스의 효율화, 핵심적 보안영역을 집중관리 할 수 있는 보안지표의 설정, 침해위험 영역을 사전 인지할 수 있는 위험지수의 산출 등을 바탕으로 한 '기업형 상시 보안관리 체계'를 연구하고, 전문가 집단의 의견을 조사하여 AHP(Analytic Hierarchy Process)방법론으로 적절성을 분석하였다. 본 연구를 통해 기업의 보안담당자들은 보안관리 체계의 운영에 있어서 선제대응, 신속조치 등의 효율성을 향상시킬 수 있다.

ABSTRACT

Many businesses have adopted the standard security management structure such as ISO27001 and K-ISMS for strengthening business's security management structure to protect their core information assets and have acquired partial output from such effort. However, many risk factors such as recent advances in Information Technology and evolution of intrusion methods have increased exponentially requiring the businesses to response even more quickly with better accuracy. For such purpose, a study of 'Real Time Security Management Structure for Business' based on security management process optimization, defining a set of security index for managing core security area and calculation of risk indices for precognition of intrusion risk area has been made. Also, a survey on opinions of an expert panel has been conducted. The effectiveness of studied structure was analyzed using AHP method as well. Using this study, security personnels of a company can improve efficiency of the preemptive responsive and quicker measure from the current security management structure.

Keywords: Security, Lifecycle, Risk, Real time, Enterprise

I. 서 론

1.1 연구목적

기업은 핵심 정보자산의 보호를 위해 외부의 보안위협에 대응이 가능하도록 '보안관리 체계'를 구축하여 운영하고 있다. 그러나 이러한 보안관리 체계가 제대로 작동하지 않을 경우 악성코드 등의 위협요인 등을 인식하지 못하거나 신속하게 대응하지 못한다면 순식간에 감염이 확산되어 기업을 큰 혼란으로 빠뜨릴 수 있고, 비즈니스에도 치명적인 영향을 초래할 수 있을 것이다. 예를 들면 2011년 발생한 해외 'S' 社 주력 게임기 및 관련 홈페이지 해킹사고의 경우, 장시간 동안 이를 인지하지 못해 대응이 지연되

Received(03. 28. 2017), Modified(05. 04. 2017), Accepted(05. 16. 2017)
† 주저자, secnsy@samsung.com
‡ 교신저자, jilim@korea.ac.kr(Corresponding author)

었고, 보상액도 눈덩이처럼 커진 것으로 알려지고 있다[1]. 또한, 법적으로 국내 'K-ISMS(Information Security Management System)' 의무도입 대상인 기업들은 한국인터넷진흥원(KISA)에 의해 인증을 받고 주기적 심사에 의해 보안수준의 지속여부를 검증받게 되는데 보안전문가들은 '전체 보안수준 향상보다는 법률에서 정한 기준에만 맞추려는 형식적 측면의 단점', '대상기업의 특성을 고려하지 않은 일률적인 정보보안 관리체계' 등으로 문제점을 지적하고 있다[2]. 본 연구에서는 이러한 보안위험의 사전인지와 신속대응을 통한 보안강화를 위해 국내 'K-ISMS'[1] 보안관리 체계'를 참조하여 보안관리 프로세스의 효율화, 침해사고 시 치명적 영향을 줄 수 있는 핵심 보안영역의 집중관리, 보안영역 별 침해위험도를 산출하여 기업전체의 보안 위험수준을 인지할 수 있는 방안 등을 제시하고자 한다.

1.2 연구방법

1.2.1 연구대상

연구의 대상은 국내의 '표준 보안관리 체계'로 인정받고 있는 'K-ISMS'와 기업들 중에서도 상대적으로 보안수준이 높은 'A'사의 보안관리 체계를 기반으로 하여 각 관리체계를 구성하고 있는 프로세스, 보안영역의 정의, 보안영역을 구성하고 있는 통제사항 등을 비교 검토하고, 보완 필요성을 도출한다.

1.2.2 연구단계

본 연구는 보안업무에 대한 경험과 현장에서 제기된 보안관리 상의 이슈사항 등을 바탕으로 1단계 선행연구에서는 기존 보안관리 체계의 효과성 및 문제점 등과 관련한 연구결과 및 보안관리 체계의 개선필요성 등을 검토하여 연구의 타당성 등을 판단하고, 2단계, 기존 보안관리 체계의 현황분석에서는 K-ISMS 관리체계와 민간기업 'A'사의 관리체계를 분석하여 보완 필요부분을 도출, 3단계에서는 바람직한 기업 보안관리 체계 모델. '상시 보안관리 체계'를 제시, AHP 방법론에 의해 그 적절성을 검증하였다.

1) K-ISMS: KISA(한국 인터넷 진흥원)주관의 ISMS 체계 및 인증제도

II. 선행연구

2.1 ISMS 개요 및 구성요소

ISMS는 "경영의 일부로서 비즈니스 Risk 중심의 정보보안 체계를 확립, 적용, 운영, 감시, 평가, 유지, 향상시키기 위한 관리체계(ISO)", "조직의 정보자산 보호를 위해 보안관리 절차와 과정을 체계적으로 수립하여 지속관리, 운영하기 위한 종합적 체계(KISA)"로 정의하고 각각 ISO27001[2], K-ISMS 표준에 따른 인증의 부여, 사후심사 등을 실행하고 있다. [3,4].

또한, ISMS는 보안정책 수립단계로부터 사후관리에 이르기까지 정책수립-범위설정-위험분석-대책적용-사후관리 등 PDCA(Plan, Do, Check, Act)형태로 진행되는 관리과정과 이러한 과정 내에 조직의 보안목표를 달성하기 위한 보안영역별 통제사항을 포함한 대책과정으로 구성되어 있는데

Table 1. K-ISMS Criteria

Management Process - 5 Step 12 Activities	Countermeasure Controls - 13 Area 92 Activities
1. Security Policy & Scope	1. Security Policy
2. Responsibility & Organization	2. Security Organization
3. Risk Management	
4. Implementing Countermeasure	3. Security of External Parties
	4. Infomation Asset Classification
	5. Security Educatuion
	6. Personal Security
	7. Physical Security
	8. Development Security
	9. Crypto. Control
	10. Access Control
	11. Operations Security
5. Post Management	12. Incident Handling
	13. IT Disaster Recovery Planning

2) ISO27001: 국제 표준화 기구(ISO)에 의해 정보보안경영시스템 개발, 수립, 문서화 요구사항을 정하여 국제표준으로 제정된 규격

K-ISMS에서는 이를 각각 '관리과정' 5단계 12개의 통제사항과 '대책과정' 13개 분야 92개 통제사항으로 분류하여 각각 관리하고 있으며 ISO27001도 이와 유사한 체계를 가지고 있다. Table 1은 K-ISMS를 구성하고 있는 각 과정별 분류 내용이다[3,4].

2.2 ISMS 문제점 관련

Haider Abbas 등은 'Addressing dynamic issues in information security management' 논문(2011)[6]에서 기존 보안관리 체계의 불확실성에 대한 3가지 이슈를 제기하였는데 첫째, Dynamic Issue, 즉 급변하는 보안요구에 대한 대응 이슈로서 급속한 기술발전은 조직에 새로운 보안 이슈를 만들 수 있으나 기존의 보안조치, 통제 등 보안관리 체계는 여기에 따라가지 못할 수 있고, 둘째, Externality Issue, 즉, 표준 보안관리 체계의 적용에 따른 외부효과 이슈로서 조직 내에서 ISMS 등 보안경영 시스템 등을 적용할 경우 보안시스템의 적용으로 인한 타 시스템에 대한 영향이 불분명하여 다른 경영체계에 악영향을 미칠 수도 있으며, 셋째, Re-Evaluation Issue, 즉, 보안수준의 평가 시 뒤떨어진 평가기준을 사용하는 것인데, 기업에서 제공하는 새로운 제품, 서비스 기술 등을 대상으로 신기술 및 새로운 취약점, 새로운 위협요인에 대한 보안문제 존재여부를 지속 평가해야 하지만 기존의 보안조치, 통제 등으로는 한계가 있을 수 있다는 점 등을 지적하였다. 즉, 사전 설정된 일률적 통제항목으로 구성된 ISMS 체계로는 급변하는 보안요구 및 새로운 위협요인에 대한 대응이 어렵기 때문에 ISMS 체계 자체가 또 다른 보안위험이 될 수도 있다는 것이다. 따라서 조직의 보안관리 체계, 즉 ISMS 체계에는 이러한 위협요인들을 상시적으로 도출할 수 있는 프로세스가 반드시 포함되어야 할 것으로 판단된다. 또한 IT 연구소 BCS사의 "Why ISO27001 is not enough?"(2009)[7]에서 "ISO27001는 보안표준이 아니라 경영표준으로서, 조직의 보안을 보장할 수 없고, 조직이 감수할 수 있는 위험 Level을 정의하지 못하므로 ISO27001이 보안을 강화하는 방법이지만 보안수준 지속유지를 위해서는 정보보안에 대한 '강력한 관리', 정보보안을 위한 Ownership, 책임, 정보보안 인식교육이 반드시 필요" 한 것으로 제언하고, "위험평가에서 감수할 수 있는 위험 Level이 정해지지 않으므로 나타난 모든 위협요소들을 통제사항에 반영해야 하는 무리함도 존재" 하고 있다고 말한다. 여기에서 주장하는 '강력한 관리' 측면에서 고려해야 할 사항들은 기존의 ISMS가 가지고 있는 절차, 과정, 통제사항 들이 보다 더 실질적이고, 세부적인 내용으로 강화, 추가 구성되어야 한다는 의미로 해석할 수 있다.

2.3 ISMS 효과성 관련

ISMS 체계가 가지고 있는 이러한 상시성 부족, 위험 Level의 도출 및 관리 미흡 등 문제점 개선을 위해 국내에서도 다음과 같이 연구가 진행되었다.

2008년 이희명은 '기업 정보보호수준 측정모델 개발에 관한 연구'에서 기업들이 ISMS를 도입하여 활용중이지만 이를 이용한 보안수준 측정 시 IT영역에 한정되거나 지표항목 및 내용의 불충분 등으로 전체 보안수준 도출이 어려운 점을 지적하고 이의 해결을 위한 방안으로서 지표를 세분하여 '기반지표'는 기업의 정보보호체계를 각 영역별로 측정하기 위한 원칙과 기준, '이행지표'는 실제 업무 수행과정에서 정보보호 규정이나 프로세스를 실천하는 정도를 측정, '결과지표'는 '기반지표'와 '이행지표'의 최종결과로써 나타나는 보안수준의 결과를 보여줄 수 있도록 함으로서 실질적인 보안관리 체계의 기반을 마련하여 객관적인 전체 보안수준을 명확히 알 수 있게 하였다고 기술하였다[8].

2011년 강신범은 '기업의 침해위협 예방을 위한 관리체계 강화방안' 연구에서 먼저 정보보호 관리체계를 도입하였다고 해서 모든 사이버 범죄를 예방할 수 없으므로 위협요인을 트래픽 공격(T), 탐색공격(R), 취약점 공격(V), 보안정책 공격(S), 네트워크 공격(N) 등으로 분리하여 해당 공격들 간의 상관관계를 분석, 하나의 위협이 발생할 경우, 뒤따를 수 있는 공격, 혹은 과거에 있었을 수도 있는 선행적 공격의 유무를 파악하고, 이에 따른 위협 유형을 주의형, 관계형, 독립형, 자원관리형으로 분류, 주의형은 R, T, N 위협으로서 내외부를 함께 관리하되, 처리기준은 모니터링과 외부기관과의 협조를 중심으로 하였고, 관계형은 V 위협으로 모니터링 및 패치, 추적관리를 중심, 독립형은 S 위협으로 하되, 케이스별 수동처리, 자원관리형은 T 위협으로 분류하고 외부기관의 협조 중심으로 처리하도록 기준이 필요할 것으로 정의하였다. 즉 위협요인의 상관관계를 분석하고 이에 따른 처리기준을 제시, 관리지표에 반영토

록 하면 보안관리 체계가 실제적으로 향후 발생할 위협요인에 대해 예방적 효과를 가질 수 있다고 언급하였다[9].

2013년 권상은은 '실시간 보안수준 측정을 위한 정보보안관리 모델 연구'에서 국내에서 활용되고 있는 보안관리 체계, 즉 K-ISMS, G-ISMS(전자정부ISMS), PIMS(개인정보ISMS) 등의 문제점으로 각 기관의 특성을 고려하지 않고 동일한 규격으로 관리체계를 적용하는 점, 정보보호 관리체계의 인증이 일시적으로서 지속적인 대응 및 관리가 불가능하여 보안의 허점이 발생하기 쉬운 점 등을 지적하고 각 기관별 특성을 고려한 통제항목과 위협요인의 상시적 관리를 위한 대시보드 시스템으로 구성된 관리체계 모델을 제시하였다[10].

2014년 고유찬은 'ISMS 인증제도의 개선을 위한 연구'에서 대상기업에 정보보호 관리체계의 모든 항목을 적용시키기 보다는 기업의 규모와 서비스 종류에 따라 필요한 부분만 적용을 시켜 비용은 물론, 관리체계의 대상을 집중할 수 있으므로 관리체계 효율성을 향상시킬 수 있다고 주장하였다[11].

2015년 이경호는 조직의 위험수준 도출에 대해 '정보보안 통제상태 평가방법 및 장치'의 특허를 등록하였는데 네트워크나 정보시스템 상에 내재하는 알려진 취약점과 알려지지 않은 취약성을 점검, 분석하여, 정보보안 위험지수를 산출 할 수 있는 방법을 제시하고, 이로서 정보보안 위험에 대한 대응책을 제공할 수 있다고 하였다[12].

2.4 상시 보안관리 체계의 필요성 및 연구방향

ISMS에 대한 문제점과 이의 해결을 위한 다양한 연구에도 불구하고 기업의 경영정보, 기술정보 탈취를 목적으로 한 최근 기업보안의 위협요인들은 다음과 같이 정리할 수 있다.

첫째는 대부분 기업에서 비즈니스 자체, 혹은 수단으로 활용하고 있는 하드웨어 및 소프트웨어의 취약점이다. 공격자들은 이러한 취약점을 이용하여, 기업의 핵심정보를 절취하기 위한 악성코드 등을 제작 유포하고 있고, 직접적인 해킹공격도 불사하고 있으며 그 빈도 및 수법도 시시각각으로 진화하고 있다. Symantec 사의 2016년 위협보고서에 따르면 하드웨어 및 소프트웨어의 취약점은 2013년 6,787건, 2014년 6,549건, 2015년 5,589건 등 매년 수천건 이상이 발견되고 있으며 특히 제조사, 또는 개발사 등이 보완조치를 하지 못한 'Zero-Day 취약점'은 매주 발견되고 있을 뿐만 아니라 2014년 24건, 2015년 54건으로 지속 증가하고 있는 것으로 나타났다[13].

둘째는 IT기기, 혹은 인터넷 사용자의 편의를 위해 신규개발, 제공되고 있는 서비스들이 오히려 기업을 위협하고 있는 복병이 되고 있다. 예를 들면 2014년 1월 전자신문의 "윈도 오류보고시스템이 해킹 위험 키운다"기사에 따르면 MS 사에서 PC Windows OS의 오류수정을 위해 인터넷에 연결된 PC에서 S/W오류가 발생할 경우 해당 PC의 IP와 OS 버전 등을 MS 연구소로 전송하고 있는데 이는 타겟 공격을 위한 훌륭한 소스정보로 오용될 수도 있다고 하였고[14], 인터넷상에서 수집한 기업의 문서를 인터넷에 무차별 공개하는 'Filemare'[15], 인터넷에 연결된 통신장비의 취약점 현황을 제공하는 'Shodan' 서비스[16]등 이와 유사한 정보 서비스 사업이 지속 증가하고 있다.

셋째로는 국가간 생존경쟁 차원에서 인터넷을 활용한 안보 및 정보활동이 증가함에 따라 기업이 선의의 피해자가 될 수도 있다는 점이다. 예를 들면 2013년 월 스트리트 저널은 반도체 칩 내에 해킹회로가 삽입되어 있을 가능성을 제기[17]하였고, 연합뉴스는 2013년 7월, 이러한 위협의 회피 목적으로 영국의 정보기관과 미국 국무부에서는 중국산 반도체칩이 포함된 레노버 PC의 사용을 금지하였다고 보도[18]한 바가 있으며, 또한 2013년 12월 독일 Spiegel Online에서는 "Documents Reveal Top NSA Hacking Unit"란 제목으로 대부분 국가가 사용하는 통신장비 및 서버에 NSA가 해킹 프로그램을 삽입한 의혹이 있다고 보도한 바가 있다[19].

따라서 기업에서 보안 사고를 예방하고 내부정보를 보호하기 위해서는 시시각각으로 나타나고 있는 다양한 위협요인에 대해 지속적인 감시, 예방조치 등의 선제대응, 실시간 사후관리가 필수적이라 하겠다.

반면 선행연구에서 조사된 기존 ISMS 체계의 문제점으로서는 급변하는 보안요구에 대한 대응이 어렵고, IT 기술 발전에 따라 통제항목도 상시적으로 진화해야 하지만 이를 쫓아가지 못하고 있으며, 기관별 특성에 따라 감수할 수 있는 위험수준 등을 감안한 위험관리도 미흡한 상태로 보았다. 또한 이의 해결을 위한 연구에서도 현재 보안수준의 실제적인 측정, 위협요인을 감안한 보안지표의 설정, 실시간 측

정을 위한 대시보드 시스템의 구축 등 상시 보안관리를 위한 근본적 해결보다는 관리체계의 정확성을 향상시키기 위한 방법에 집중하고 있었다. 따라서 본 논문에서는 선행연구를 바탕으로 상시적으로 위험영역을 도출할 수 있고, 보안지표의 정밀화 등을 통해 위험요인을 사전 표출함으로서 선제대응이 가능할 수 있도록 '기업형 상시 보안관리 체계'를 제안한다.

III. 기업 보안관리 체계 현황

3.1 K-ISMS 분석

정부는 2002년 'K-ISMS 보안관리 체계 인증제도' (Information Security Management System)를 도입하여 기업이 일정규모 이상의 인터넷, 개인정보 관련 비즈니스를 하게 되면 의무적으로 'K-ISMS 인증'을 받도록 하였고, 2013년에는 IT 신기술 트렌드를 반영, 유사기준을 통합하고, 실효성 낮은 기준을 삭제하는 등의 개정작업을 추진한 바가 있다[4]. 이에 K-ISMS의 관리과정 5단계와 대책과정 13개 분야의 통제사항에 대해 현장에서의 영향 및 효과성 등을 분석하기 위해 2014 ~ 2016 3년간 K-ISMS 관리체계의 인증을 취득한 'A'사의 보안 담당자들과 공동으로 K-ISMS 관리체계의 효과성, 문제점, 개선의견 등에 대한 검토 작업을 하였고, 분석내용은 다음과 같다.

3.1.1 정보보호 관리과정 5단계

아래 Table2와 같이 K-ISMS의 정보보호 관리과정 5 단계는 조직 내에서 보안관리 활동의 절차를 정책과 범위설정, 책임할당과 조직구성, 위험분석, 대책적용, 사후관리 등 5단계로 정의하고 주기적 운영을 하도록 하여 도입 기업들이 지속적 보안활동에 의해 보안수준의 향상도 이루어질 수 있게 하였다[5].

Table 2. K-ISMS Managenet Process 5 steps

No.	MAIN CONTENTS
1	Establishment of Information Security policy & scope
2	Define that management have to participate allocating resource for IS
3	Analyzing vulnerabilities and risks which resides in an organization
4	Implementation of Information security countermeasure
5	Review, monitor, upgrade of IS contermeasure implemented

반면, 현장에서는 정보보호 관리과정 5단계의 보완 필요성을 다음과 같이 제기하였다. 첫째, "관리과정 5단계로서는 기업현장에서 발생하는 보안 전반적인 활동단계를 반영하기가 어렵다"는 의견이 도출되었다. 즉 기업에서 보안정책 및 전략을 수립하기 위해서는 먼저 핵심 정보자산의 정의, 이 핵심 자산에 대한 관리정책 및 보호대책, 정책에 대한 compliance의 검토 등이 선행되어야 하고, 확정된 보안정책 등에 대해서도 구성원간의 공유를 위해, 교육 및 홍보 활동 등이 필요하며, 보호대책의 경우에도 사전 충분한 검증이 이루어져야 한다. 따라서 관리과정의 실질적인 현장 반영을 위해서는 5단계보다 더 세분화되고 구체적 단계의 정의가 필요할 것으로 조사되었으며, 관리과정과 대책과정을 별도 관리해야 하는 어려움도 제기되었다. 둘째, 관리과정 5단계의 통제사항에서는 의미상 대책과정 통제사항과 중복될 경우가 있어 이의 정리가 필요한 것으로 파악되었다. 예로서 Table 3.과 같이 '보안정책 수립' 항목의 경우, '최상위 수준의 정보보호정책의 존재' 여부를 체크하는데 이는 대책과정에서 '정보보호정책의 최고경영자 승인여부' 항목과 유사하였다[5]

이와 같이 통제사항의 일부 내용들은 대책과정의 13개 분야에서 확인할 수 있거나 부연 설명으로 간주되어도 좋을 내용이어서 정보보호 대책과정과의 통합운영, 또는 관리과정을 세분화하여 실제 현장의 보안업무 라이프사이클과 1:1로 합치시키는 방법 등으로 일원화, 단순화 필요성이 제기되었다.

Table 3. Example of the approximate equivalent activities between management process and countermeasure control

Management Process	Countermeasure Controls
Policy Establishment	Policy Approval
Check the existence of top level policy	Need the approval of top management

3.1.2 정보보호 대책과정 13개영역

정보보호 대책과정의 경우 보안 담당자들은 '각 분

야의 상세한 통제사항들을 학습할 수 있고, 실제 보안수준의 유지에 필요한 대책내용 들을 참고할 수 있어서 많은 도움이 되었다'라는 언급하고 일부 보완 및 조정 필요성이 있는 내용을 다음과 같이 제기하였다.

첫째, ISMS는 보안관리 체계인데도 불구하고 정보시스템 분야의 자원관리 및 재해복구 부분 등을 포함하고 있는 등, 순수 보안측면으로 통제내용이 집약되면 좋겠다는 의견이 있었다. 이는 기업에서 업무의 책임범위 문제와도 많은 연관이 있으므로 IT부문의 자원관리 업무는 보안부문이 아니라 IT 분야의 책임으로서 별도 관리가 필요하다는 의미이다.

둘째, 기업의 정보자산 보호를 위한 보안관리 체계는 기업 내에서 특정분야에 국한되지 않고 기업 전체 범위를 포함해야 하므로 물리적 보안의 경우에도 일부 IT시설뿐만이 아니라 기업 전체의 시설분야를 포함해야 한다는 의견도 제기되었고, 그 외에는 각 보안영역 별 통제사항의 내용을 구체화, '외부자' 등 용어의 변경, 각 영역 별 통제사항의 귀속영역 변경 요구 등이 있었으며, 요약내용은 다음 표와 같다.

Table 4. The need to improve of Countermeasure controls

Controls	Need to improve
Policy	Actual guide of Legal validity and the admissibility of evidence about policy
An outsider	Changing of the term and moving to IT area
Education	Including Security Personnel
Physical Security	Changing to the "Facility Security" and including entire company
Development, Crypto, Access Control	Integrating to the "System Security"
IT operations, Disaster recovery	Moving to the other management area not the security management

3.1.3 K-ISMS 검토내용 요약

K-ISMS의 관리과정과 대책과정에 관한 현장 실무자의 의견을 요약하여 먼저 긍정적 측면의 내용을 다음과 같이 정리하였다.

① 법적 준수사항 등의 주기적 검토, 보안업무의 역할 에 대한 R&R을 구체화 하는 등 신속한 대응을 할 수 있는 관리체계의 구축에 많은 도움을 받음.
② 전체적인 보안관리 업무와 프로세스를 경험할 수 있어 보안지식, 점검능력 등 기술수준 향상을 지원.
③ 인증취득 및 유지 과정에서 경영진 인식제고, 투자 활성화, 임직원의 보안대책에 대한 인식제고 등의 효과 등으로서 이는 KISA의 2007년 "정보보호 실태조사[34]" 및 2013년 장상수의 "정보보호관리체계 운용이 정보보호 성과에 미치는 영향[35]"연구에서도 나타난 바와 같이 보안강화는 물론 경제적 효과까지 얻고 있다는 결과와도 일맥상통한다.

반면 보완이 필요한 내용은 다음 사항들로 나타났다.

① 현재시점 기업의 전반적 보안관리 상태에 대한 점검은 될 수 있으나 모의해킹, 침투테스트 등을 통한 '안전한지'에 대한 확신은 미흡하므로 이러한 위험여부를 파악할 수 있는 방법,
② 관리과정과 통제과정의 중복부분, 과정별 통제사항에 대한 기업현황을 반영한 내용 등에 대한 조정과 관리과정의 각 단계를 기업에서 수행되고 있는 보안활동 라이프사이클에 합치시킬 수 있는 방안,
③ 제조, 금융 등 유형에 따라 K-ISMS의 통제사항 외 추가적으로 필요한 보안대책의 조정 방안,
④ 위협요인에 대해 신속히 파악, 조치를 할 수 있는 '모니터링' 영역의 강화방안 필요 등으로 집약되었다.

이와 같이 K-ISMS에 대해서 현장에서는 실제 위협요인의 확인, 업무 프로세스와의 일치, 모니터링 영역의 강화 등이 필요한 것으로 나타났는데, 보안컨설턴트 강은성은 칼럼에서 "ISMS는 정보자산의 보안위험을 평가하고 이에 대한 대책을 수립, 시행하는 체계를 갖추는 것에 핵심목적이 있고, 정보보안은 결국 기업 스스로 해 나가야 할 문제"로서 ISMS가 실제 위협요인의 발굴 등은 어렵다는 것을 언급한 바가 있고[20,21], 빛스캔사 문일준은 언론기고에서 "웹사이트의 경우 컨텐츠 등이 끊임없이 추가되고 수정되는 생명체 같이 움직이므로 시간이 지남에 따라

여러 가지 문제점이 발생할 수 있으나 관리체계 자체는 따라갈 수 없다"(2013)는 점을 지적하였다[22].

즉, 현재의 K-ISMS 체계가 실질적 위협요인의 발굴과 실제적 보안수준 확인은 어렵다고 보고 있기 때문에 모니터링을 통해 조직의 보안 위험도를 알려줄 수 있는 보안지수, 즉 위험지수와 이러한 위험지수를 산출해 낼 수 있는 보안지표 등의 활용으로 보완할 수 있을 것으로 판단된다.

'모니터링 체계'의 경우 2016년 임채호 전 KAIST 교수는 보안뉴스 기고를 통해서 위협요인의 상시 발굴을 위해서는 조직의 보안상태에 대한 지속적 관찰 및 인식이 이루어져야 하는데 미국 NIST의 'Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations' (2011) 보고서[23]를 인용하여

- 보안 상태를 표시할 수 있는 Metrics 정의
- 모든 보안통제는 지속적인 효과성을 확보
- 법적 준수(Compliance) 검증
- 전체 정보자산에 적용되어야 하며 지속인식 등의

6가지 ISCM 전략의 실행이 필요한 것으로 언급하고, '지속적 감시체제(Monitoring)'의 효과적 구축 및 활용을 위해서는 정보 수집을 자동화할 수 있는 시스템 구축사용도 권장하였다[24].

3.2 'A'사 보안관리 체계 분석

기업들은 일반적으로 보안업무의 목표를 KPI(Key Performance Indicator)형태로 설정하고 이를 달성하기 위해 PDCA(Plan-Do-Check-Act) 방식으로 보안관리 체계를 운영하고 있다. 예를 들면 KPI Institute는 '2011~2012 Top 25 IT Security KPIs' 에서 IT Security 분야의 Top-5 KPI를 '비즈니스 목표와 보안목표의 일치율', 'Compliance 준수율', '물리적 보안 침해로 인한 보안사고 건수', '비즈니스에 영향을 준 정보보안 사고 건수', '최신 백신 설치율' 등으로 정리[25]하였는데 이들은 기업에서 정하는 내용과 크게 다르지 않다. 다만, 이러한 KPI들은 보안사고가 발생하면 CEO, 혹은 CSO에 의해 임의로 정해지는 경우가 많아 부정적 영향을 끼칠 수도 있는데 경영컨설팅 전문 'In Future'사의 유정식은 본인 블로그에서 KPI체계의 부정적 효과로서

- 정성적 측면의 성과들을 외면 우려
- 낮은 목표치의 KPI로 인해 도전의욕 저하
- 1년 단위의 단기적 성과를 위주로 측정
- 사전 KPI 설정으로 유연한 대응 곤란 등을

언급하고 해결책으로서는 '상시 피드백'과 '상시 검토'를 강조하며 이러한 체계를 위해서는 시스템적인 뒷받침이 되어야 한다고 말하고 있다[26].

KPI 관리체계의 단점을 보완하기 위해 일부 기업에서는 '보안지수' 개념의 관리체계를 구축하기 시작하였다. '보안지수'(또는 정보보호지수[27])는 "보안을 구성하는 각종 보안지표, 즉, 보안정책의 수립여부, 보안 솔루션의 정상 사용여부 등 현재 보안상태를 나타낼 수 있는 지표들을 측정하여 목표 보안수준과 비교할 수 있도록 현재상태를 나타내는 수치"로 정의할 수 있고, 이러한 관리체계는 조직의 전반적 보안수준, 개선 여부를 파악할 수 있어 KPI 체계의 단점을 개선할 수 있다.

3.2.1 'A'사 보안지수 관리체계 개요

'A'사 '보안지수' 관리체계의 특징은 보안범위를 전체조직으로 확대하고, 보안등급에 의해 보안수준을

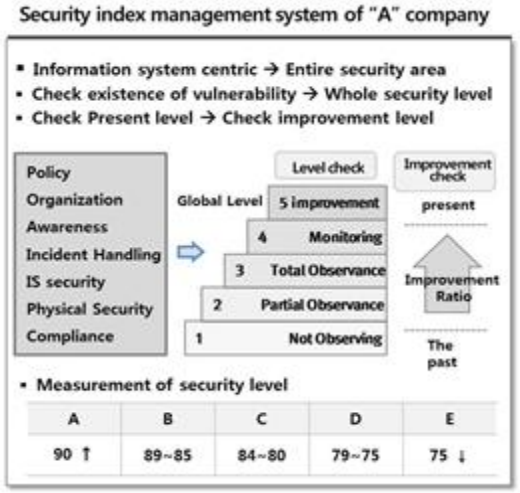


Fig. 1. Security Index Management System of "A" Company

인식할 수 있게 하였다. 또한 각 통제사항별 5단계 목표수준과 함께 위험수준을 설정하여 위험관리 및 단계별 향상여부도 관리하여 지속적 개선노력을 유도하였다.

이렇게 'A'사의 보안지수 관리체계는 효과적인 보안활동을 할 수 있게 하였지만 여전히 즉시 보완이 필요한 위험, 즉 영역별 위협요인 들의 조기인식 및 선제대응 등에는 어려움이 있었으며, 이는 앞으로의 개선과제라고 할 수 있을 것이다.

3.3 보안관리 체계의 개선방향

지금까지 K-ISMS, 국내 'A'사의 보안지수 관리체계 등을 살펴보고 장단점을 분석하였다. 결론적으로 바람직한 보안관리 체계는 위협요인을 사전에 상시적으로 잘 파악하여, 신속한 대응책을 수립할 수 있고, 이를 위한 지속적인 보안활동이 이루어지게 하는 것이 관건이라고 하겠다.

분석결과와 현장 담당자들의 의견을 바탕으로 기업에 적합한 보안관리 체계의 개선방향을

1) 보안상 위협요인을 신속하게 감지할 수 있도록 관리와 통제 등의 보안업무 라이프사이클을 통합, 일원화
2) 전체적인 보안수준과 영역별 위험을 도출할 수 있도록 보안지수 및 보안지표 개념을 도입하고, 중요도에 따른 '동적지표'와 '일반지표', 위험유형에 따라 '침입위험지표', '유출위험지표'로 구분하고, 이에 의한 '종합위험지수'를 산출.
3) 상시적 위험요인의 탐지 및 대응이 가능하도록 각종 로그기록의 수집 자동화, 침해징후의 탐지 등 모니터링 지원시스템의 활용 등으로 설정하고 다음 4장의 '기업형 상시 보안관리 체계의 수립'에서 상세 내용을 다루고자 한다.

IV. 기업형 상시 보안관리 체계의 수립

4.1 보안업무 라이프사이클 체계의 정립

3장에서 살펴본 바와 같이 K-ISMS의 경우, 관리과정에서는 보안관리 체계의 프로세스를, 대책과정에서는 각 보안영역 별 통제사항을 정의하여 보안대책에 반영하고 있고, 각 대책과정의 통제사항들을 관리과정의 프로세스에 의해 시행될 수 있도록 하고 있다. 그러나 실제 현장에서는 이들을 별도의 관리업무로 간주하고 있어 프로세스와 대책의 구현을 분리하지 않고, 통합 일원화하여 진행할 수 있다면 보안관리 체계가 보다 더 효율적으로 운영될 수 있을 것이다. 'A'사에서는 일부 의무적으로 K-ISMS 체계를 도입하여 인증을 받고 있는 영역도 있지만 그 외의 영역에 대해서는 관리 프로세스와 보안대책의 적용 등을 통합, 일원화하여 관리체계를 운영하고 있다.

Fig 2.는 'A'사의 보안업무 라이프사이클을 참조하여 바람직한 라이프사이클 단계를 나타낸 그림으로서 K-ISMS의 관리과정과 대책과정을 통합하여 '① 핵심자산 분석(Crown Jewel Analysis)' 단계부터 '⑩ 점검평가 및 피드백 (Check & Assessment)' 단계까지 순차적, 수시로 실행되고, 단계별 통제사항들은 다음 설명과 같이 보안지표화 하여 운영될 수 있다.

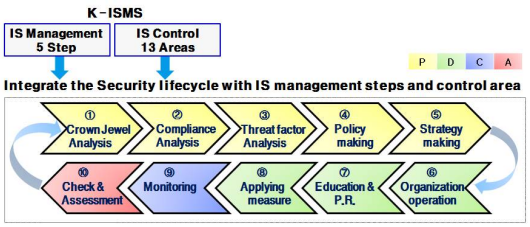


Fig. 2. Example of Integrated Information Security Lifecycle Management System

① 핵심자산 분석(Crown Jewel analysis)

기업의 보안에서 가장 우선적으로 해야 할 일은 '무엇을 지킬 것인가?' 이다. 즉, 핵심자산을 선정하는 것이다. 집중적으로 보안해야 할 대상을 파악하고 적절한 보안대책을 수립하는 것이 무엇보다도 중요하다. 또한, 기업은 항상 협력회사, 금융회사 등과 연결되어 있기 때문에 3)***핵심자산이 연관된 흐름을 파악**하여 이 과정에서 사고가 발생하지 않도록 관리해야 한다.

② Compliance 분석(Compliance analysis)

다음은 위법하지 않도록 하는 것이다. 예를 들어 보안관리 체계의 경우, '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서 일정규모 이상의 회원과 거래실적을 보유한 인터넷 서비스 웹사이트의 경우, 반드시 K-ISMS 보안관리 체계 인증을 받도록 하고

3) '*' 표시는 핵심적 관리지표, 즉 동적지표로 선정필요 항목

〔4〕, '개인정보보호법'에서는 고객의 개인정보를 암호화 저장하도록 강제〔28〕하고 있다. 또한 미국에서는 쿠키 내에 저장된 인터넷 접속이력의 활용에도 사전 동의를 받아야 하며〔29〕 러시아에서는 '15.11월부터 자국민의 개인정보가 저장된 서버는 러시아 영토 내에 둘 것을 의무화〔30〕하고, EU에서도 처벌을 강화하는 등〔31〕 Compliance의 범위가 확대되고, 위반 시 처벌도 수위가 높아지고 있다. ***국내외의 법적인 통제사항에 대해 준수리스트를 운영**하는 것도 방법이다.

③ 위협요인 분석(Threat analysis)

보안 측면에서의 위협요인은 사회적, 기술적, 때로는 정치적 환경 변화에 따라 해마다 증가, 진화하고 있고, 그 수법이 날로 지능화하고 있다. 따라서 기업에서는 ***모의해킹, 모의침투** 등으로 이러한 위협요인 들을 상시적으로 분석하여 보안정책과 전략에 반영하고, 적절한 보안대책을 적용하여 선제 대응할 수 있어야 할 것이다.

④ 보안정책 수립(Security policy making)

'보안정책'은 "기업 내부의 중요기술과 정보를 보호하기 위해 회사 및 경영진, 임직원이 업무 중 준수해야 하는 원칙과 기준"이다. 보안정책이 가져야 할 조건으로서는 정책을 실행해야 할 임직원들이 정확하게 이해를 할 수 있어야 하며, 또한 관련조직간 보안의 역할과 책임이 명확하게 기술되어야 하고, 보안정책 자체가 법적인 타당성을 반드시 가져야 한다. 즉, 내외부에서 문제가 발생하여 소송 등이 진행되더라도 보안정책이 법적인 효력을 발생할 수 있도록 사전 법무검토를 실행하여 법률에 위배되지 않도록 작성되어야 한다.

⑤ 보안전략의 수립 (Security strategy making)

이와 같은 보안정책은 반드시 기업의 보안전략과 병행하여 수립되어야 한다. 즉, 보안전략은 수립된 보안정책의 달성방법이 될 수도 있고, 보안정책은 보안전략을 실행하기 위한 도구가 될 수도 있을 것이다. 보안전략의 수립에 있어서 중요한 사항은 반드시 경영자의 경영전략과 상호 합치해야 하는 것이다. 경영자가 만약 재택근무, 모바일 근무 등 임직원들의 자유로운 업무 분위기 조성을 경영방침으로 내세운다면 보안정책과 보안전략도 이에 걸맞게 수립되어야 할 것이며 그렇지 않을 경우 보안은 반드시 실패할 수 밖에 없을 것이다.

⑥ 보안조직의 운영 (Organization operation)

보안조직은 보안정책과 전략의 실행 주체로서 보안관리 체계의 성공을 위해 가장 중요한 요소이다. 따라서 '어떤 ***전문성을 가진 사람을 조직에 포함**시켜 활용할 것인가' 하는 것은 보안의 CSF[4]라고 할 수 있다.

미국의 민간연구소인 [5]RAND Corporation과 통신장비 회사인 '쥬니퍼 네트웍스'가 공동으로 연구한 'The Defender's Dilemma : Charting a Course Toward Cybersecurity' 에서 기업들이 보안투자를 위해 고려해야 할 5가지 항목 중 하나로서 보안인력에 대한 투자를 언급하고, 보안담당자의 추가 고용 및 교육 등 투자를 통해 효과적 조직을 갖춘 기업은 첫해에 사이버보안 비용을 19%, 10년 후에는 28%까지 절감할 수 있다고 주장하였다〔32〕. 또한 보안조직은 금융, 제조 등 *소속한 기업의 특성에 적합하도록 구성해야 하며, 조직에 속한 *보안인력의 Vision 관리도 중요하다. 조직 구성원이 장기적으로 개인의 Career Path를 확신할 때 조직의 성과도 최대로 발휘할 수 있다.

⑦ 보안교육 및 홍보 (Education & P.R.)

국내외의 각종 보안사고 통계를 보면 사고 주체가 전·현직 임직원, 협력회사 등 주로 내부자에 의한 보안사고가 집중적으로 일어나고 있다. 따라서 기업의 보안사고 예방을 위해서는 임직원을 대상으로 한 보안교육과 홍보가 보안사고를 줄이는데 큰 역할을 하고 있으며 임직원 대상의 교육에서 가장 중요하게 고려해야 할 사항은 ***보안정책에 대한 이해**, 미 준수 시 불이익 인식, 교육의 정기적이고 지속적인 실행이다. 결국 보안교육과 홍보에서 가장 중요한 것은 임직원들이 '왜 보안을 해야 하는지?'"에 대한 의문을 가지지 않게 하는 것이고 생활화하기 위한 홍보가 되어야 한다.

⑧ 보안대책 구현(Applying measure)

보안대책의 핵심은 ***보안정책과 전략의 내용 전체에 대한 Coverage**이다. 즉, 보안정책에서 규정한 내용을 보안현장에서는 이를 방치해 둔다면 보안

4) Critical Success Factor
5) 미국 국방·행정 분야의 전문 Think Tank

정책의 신뢰성은 물론 보안체계 자체가 흔들리게 될 수도 있을 것이다. 조직 전체의 Coverage를 높이기 위한 방법은 보안대상 영역을 보안정책과 전략, 해당 기업의 특성에 맞게끔 분류하는 일이다. 전통적인 분류방법인 '물리적 보안', '기술적 보안', '관리적 보안', '인적 보안' 등으로 구분하는 방법이 있고, 보안을 해야 할 대상을 중심으로 핵심정보의 '내부유출 차단', '외부해킹 차단', '암호화 저장' 등으로 구분할 수 있겠고, 금융회사의 경우는 '개인정보'를 중심으로 분류할 수도 있다.

다음은 ***보안대책의 철저한 사전 검증**이다. 보안대책 적용 시 임직원들의 불만이 생기지 않게끔 성능, 효과 등에 대한 철저한 검증으로 구현 이후에 발생할 수 있는 문제점들을 제거하여 보안대책에 대한 신뢰성을 높여야 임직원, 또는 경영층 지지를 받을 수 있다.

⑨ 모니터링 (Monitoring)

모니터링 단계의 주요 목표는 실행된 ***보안대책의 정상가동 여부를 지속적으로 확인**하는 것이다. 즉 앞에서 예를 든 기업 보안 라이프사이클 각 단계별 가동상태를 체크하고 보완이 필요한 부분, 또는 새로운 보안대책이 적용되어야 할 필요성 등을 주기적으로 파악, 분석, 도출하는 것이다.

다음은 Monitoring을 정책에 반영한 예시이다.

- 자동화 도구를 사용하여 인터넷, LAN트래픽과 OS parameter의 이상여부를 실시간 탐지
- 주기적으로 방화벽, 인터넷기록, 시스템에러, 응용 프로그램 등의 로그파일을 체크하여 취약점의 존재, 혹은 잘못 사용되고 있는 징후파악 등의 실행.

⑩ 점검평가 및 피드백 (Check & Assessment)

점검평가 단계는 기업 내에서 실제로 적용된 보안수준을 확인하기 위한 단계이다. 아무리 훌륭한 보안정책과 전략을 만들고 우수한 보안 솔루션을 도입하여 적용했다 하더라도 현장에서 이를 정상적으로 운영하지 않는다면 아무런 소용이 없다. 따라서 정기, 혹은 수시로 보안적용 상태를 체크하여 미비점을 보완하고, 또 새로 발견되는 위협요인에 대해서는 보안대책을 수립하는 등의 ***점검활동을 지속적으로 실시**해야 당초 계획한 보안수준을 유지할 수 있을 것이다. 이러한 라이프사이클 단계는 금융, 제조 등의 기업유형, 연구개발, 서비스 등의 기업특성 및 필요에 따라 조정할 수도 있다.

4.2 라이프사이클 단계별 보안지표의 선정

4.2.1 보안지표의 선정원칙

4.1절에서 보안업무의 통합 라이프사이클의 10단계를 정의하였는데, 각 라이프사이클 단계별 지속적인 이행여부 및 이행수준을 확인하기 위해서는 해당 단계별 보안영역의 보안상태를 나타낼 수 있는 보안지표들이 필요하게 된다.

이러한 보안지표는

① 보안 담당자들이 쉽게 파악 가능
② 해당 영역의 현재 보안 상태를 정확하게 표현
③ 영역별 대표성, 객관성, 적시성, 차별성 보유[33]
④ 문서가 아닌 실제 상태를 확인
⑤ 보안지표 간 보안성 Level의 균등화 등

5가지의 전제조건을 가지고, K-ISMS와 'A'사의 통제항목을 참고하여 선정하였다.

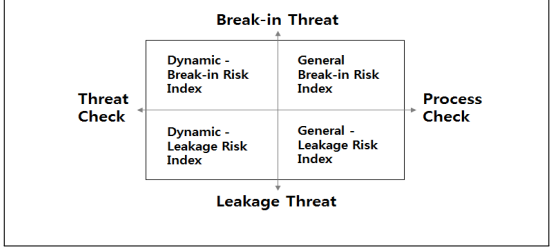
4.2.2 보안지표의 분류 및 선정

먼저 보안지표를 '일반지표(General index)'와 '동적지표(Dynamic index)'로 구분하였다. '일반지표'는 "정기적인 보안점검의 실행여부" 등과 같이 각 라이프사이클 단계별 보안영역의 통제사항 관리여부를 체크할 수 있는 항목 중심으로 선정하고, '동적지표'는 "인터넷 서비스 중인 웹사이트 내 해킹취약점의 존재여부" 등 실제 침해위험을 판별하기 위한 목적, 즉 침입, 유출 등 사고와 직결될 수 있는 통제사항과 웹사이트와 같이 수시로 운영상태가 변화할 수 있는 대상 등 상시 모니터링이 필요한 항목을 선정하였다.

다음, 실제 현장에서의 위험을 직접적으로 나타내기 위해 '침입위험지표(Break-in Risk Index)'와 '유출위험지표(Leakage Risk Index)'로 구분하였는데 이러한 분류에 의해 외부침입 위험도와 내부유출 위험도를 산출, 비교함으로서 향후 보안전략에 반영하기 위함이다. 즉 '침입위험지표'는 보안지표 중 해킹, 외부자 침입을 방어하기 위한 보안지표로 하였

Table 5. Example of the 'General index' and ' Dynamic index'

General index	Dynamic index
Operating asset classification	Identifying Crown jewel asset
Periodic checking of compliance	Operating domestic & foreign compliance list
Operating access control standard	Applying access control for servers
Periodic checking of service Web site	Removing vulnerability of Web site



고, '유출위험지표'는 주로 임직원, 협력회사 직원 등의 내부자와 정보의 유출위험을 차단할 수 있는 보안지표를 선정하였다.

마지막으로 지표 간 중복사항의 통합, 지표 중 보안직접 관련사항 외의 내용은 배제, 각 지표간 보안성 Level의 균등화 등에 의한 검토과정을 거쳐서 최종적으로는 '일반지표' 111개, '동적지표' 49개를 포함한 보안지표 160개를 선정하였고, 전체 보안지표의 분류 및 선정현황은 다음과 같다.

Lifecycle step		Security Index D	G	Tot.	Major Contents
Crown Jewel		3	5	8	Information property classification
Compliance		2	3	5	Legal compliance arrangement
Threat Anal.		3	2	5	Current threat factor arrangement
Policy, Strategy		3	7	10	Legal effectiveness of policy
Organization		3	7	10	R&R definition, Specialist
Edu. & P.R.		3	10	13	Understanding policy, measure
Applying Measure	Physical	3	6	9	Identification & mgnt. Of facilities
	IT	20	55	75	Information system security
	Product	3	2	5	Security of productions
	Incident	3	7	10	Manual existence, understanding
Monitoring		2	3	5	Security situation control
Check, Assessment		1	4	5	Checklist, Feedback process
Total		49	111	160	

Fig. 3. Set-up Result of Security Index selection of each Lifecycle Step.('D':dynamic, 'G':General)

4.3 보안지표에 의한 위험지수의 산출

위험지수의 산출은 보안지표, 즉 '일반지표'와 '동적지표'의 이행수준을 측정하여 산출하게 되는데, 각 지표의 이행수준이 일정기준 이하, 다시 말하면 심각한 침해위협이 존재하고 있을 경우, '위험'으로 분류하여 위험점수 '1'점을 부여하고, 만약 이 지표가 '동적지표'일 경우에는 지표의 중요성을 감안하여 2배의 가중치를 준 '2'점을 부여하였다.

최종적으로는 산출된 각 보안지표의 위험점수를 합산하여 백분율로 환산, 조직 전체의 '종합위험지수'"를 산출하게 된다. 다음은 보안지표의 위험점수 산출과정이다.

① 보안지표 고유특성을 나타내는 '보안지표 정의서'를 다음과 같이 작성한다. '보안지표 정의서'는 해당되는 보안지표의 목적 및 내용정의와 함께, 측정결과를 5단계의 이행수준으로 구분하여 침입 및 유출 위험 군에 속하는지, 일반지표인지, 동적지표인지, '위험점수'는 5단계의 이행수준 중에서 어떤 단계까지 이행 시 부여되는지 등과 측정 시 참고해야 할 사항 등을 정리한다.

② '보안지표 정의서'에 의해서 위험점수를 산출한다. 예를 든 '보안정책의 법적효력 확보'항목을 측정한다면,

Area	Security Policy	Goal	- legal validity in the company, - admissibility of evidence in an outside	
Index	Legal effectiveness of security policy			
ID	B.8.3			
Subject	Implementing the CEO approval, legal analysis and official regulation of security policy			
Appl y level	1	Approval of security manager		
	2	Approval of CSO(Chief Security Officer)		
	3	Approval of CEO		
	4	Approval of the Board of Director		
	5	Including in the Regulation of Employee of company		
Way of Measure	[Checkpoint] - Policy approval documents of CEO, Board of director - CEO comment about security - Documents about policy review of legal department [How to check] - Direct validation of base documents - Direct validation of employee understanding level			
Characteristics	Leakage & Dynamic risk index, classifying to 'danger' if under level 3			
Etc.	Legal review is the essential point of each level			

Fig. 4. Example of Security Index Definition form

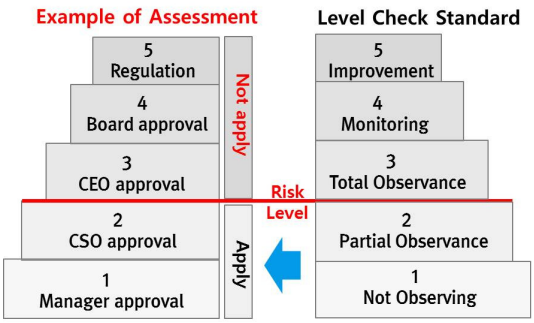


Fig. 5. Example of Measurement of one of the Security Index

보안정책이 사내, 혹은 대외에서 법적인 효력을 갖추기 위해서는 CEO의 승인은 기본이고, 이사회의 승인, 취업규칙 화까지 진행되어야 완벽한 법적 효력을 갖출 수 있다. 그러나 보안부서장, 또는 CSO의 승인만으로는 법적인 효력요건이 되지 않으므로 이 보안지표는 '위험'으로 간주되고 또한 '동적지표'이므로 2배의 가중치를 부여하여 위험점수 '2'점이 부여되게 된다.

③ 측정된 각 보안지표들의 위험점수를 합산하여 조직전체의 '종합위험지수', '침입위험지수', '유출위험지수' 등을 산출하게 되는데 산출결과는 백분율로 환산하여 표시한다. 즉 보안이 위험한 상태를 백점으로 간주하고, 종합위험지수가 40점이 산출되었다면 위험수준이 40%가 되고, 이중 침입위험은 30%, 유출위험은 10% 등으로 나타내게 된다.

이를 수식으로 표시하면

G(General)는 일반지표, D(Dynamic)는 동적지표, B(Break-in)는 침입위험지표, L(Leakage)는 유출위험지표, R(Risk)은 위험점수 값으로 정의하고,

침입위험지수 BRI(Break-in Risk Index)는 일반지표 중 '위험'으로 측정된 침입위험지표의 개수와 동적지표 중 '위험'으로 측정된 침입위험지표 개수의 2배를 합산하여 일반지표 개수와 동적지표 개수의 2배를 합한 전체 보안지표의 위험점수로 나누고 백분율로 환산한다. 유출위험지수 LRI(Leakage Risk Index), 종합위험지수 SRI(Security risk index)도 이와 같은 방법으로 다음 수식에 의해 산출되게 된다.

$$SRI = \frac{\sum_{i=1}^{G} R(i) + (2 \times \sum_{i=1}^{D} R(i))}{G + 2D} \times 100$$

$$BRI = \frac{\sum_{i=1}^{BG} R(i) + (2 \times \sum_{i=1}^{BD} R(i))}{BG + 2BD} \times 100$$

$$LRI = \frac{\sum_{i=1}^{LG} R(i) + (2 \times \sum_{i=1}^{LD} R(i))}{LG + 2LD} \times 100$$

이렇게 산출된 조직의 '종합위험지수'는 역으로 침입과 유출, 또는 각 보안영역별, 또는 보안지표 별 분해하여 위험이 도출된 부분은 즉시 보완할 수 있다.

4.4 보안지표 정보의 수집을 자동화

각 보안지표들은 하나의 보안지표 정의서, 또는 여러 개의 부속 체크리스트가 필요할 수도 있다. 즉 모든 보안지표와 그에 부속되는 또 다른 하위의 모든 체크리스트를 조합하면 극단적으로는 수백, 수천 개의 체크항목을 점검해야 하는 경우도 발생할 수 있다. 따라서 이러한 지표정보의 수집과정을 자동화하지 않으면 '상시적'인 보안관리 체계의 운영은 불가능하다. 보안지표의 특성에 따라서는 시스템화가 가능하지 않을 경우도 있을 것이나 가능한 부분을 최대한 포함시키고, 점진적으로 그 범위를 확대해 나가야 한다. 이러한 시스템화 비율을 관리체계 내에 보안지표로 포함시키는 것도 좋은 방법이 될 수 있다. 'A'사에서는 수량이 많은 서버, PC 등은 자동점검 툴을 이용하고, 보안정책의 운영여부 등 자동화 할 수 없는 부분은 점검 담당자가 입력하게 하여 자체점검, 이력관리, 통계현황 등의 기능으로 각 영역을 주기적, 상시적으로 점검, 분석된 결과를 시스템에 저장하여 지속관리가 가능하게 운영하고 있다.

이러한 지표정보의 직접적인 자동화 방법 외에 또 한 가지의 방법은 시스템에 의해 이상상황에 대한 징후를 사전 인지할 수 있도록 '보안사고 징후탐지 시스템'을 구축하여 탐지된 정보를 보안지표에 활용하는 방법이 있다. 조직에서 사용하는 통신장비, 서버 및 PC, 또한 각종 보안시스템 등에는 업무시간 동안 사용하는 통신 트래픽, 서버 및 PC의 접근기록, 인터넷 관련 정보 등이 로그파일에 설정한 기간 동안 보관된다. 여기에는 로그인 기록, 접속시간, 접속실패 정보, 침입시도 정보, 사용내역 등의 다양한 정보가 보관되어 있고, 집적된 정보를 빅 데이터 기

법으로 분석하여 숨겨진 위협요인을 찾아내는 방법이다. 예를 들면, 외부의 특정 IP에서 인터넷 서비스 홈페이지에 1~2분 동안의 짧은 시간에 수천 수만 번의 로그인을 시도하고 있다면 이를 기록한 방화벽의 로그파일에서 동일한 패턴을 추출하여 해킹 수법의 일종인 'Brute Force' 공격으로 간주하고, 감지되는 즉시 해당 IP를 차단하여 위험을 회피할 수 있고, 이와 같은 관리 시스템을 관리체계의 '모니터링' 영역에 반영한다면 위험을 조기인식할 수 있을 것이다.

'A'사 에서는 '빅 데이터 Analytics' 기법을 활용한 '징후탐지 시스템'을 구축하여 활용 중으로서 기계학습(Machine Learning)을 통해 보안 특이점(Outlier)을 분류 (Clustering) 또는 탐지(Detection)하거나 과거의 악성 또는 위험 행위를 학습한 후 유사 공격행위, 경향을 탐지하는 시스템으로서 해킹, 악성코드 감염, 정보유출 등에 관한 표준 시나리오를 설정하여 해당 시나리오의 징후가 포착될 경우, 확인절차를 진행한다. 이런 방식으로 상시 위협요인을 발굴하여 조치함으로서 사고의 사전예방 또는 확산을 방지하는 효과를 거둘 수 있다.

4.5 기업형 상시 보안관리 체계의 설계

'기업형 상시 보안관리 체계'의 목표는 현재시점에서 조직의 보안 수준이 어느 정도인지, 또한 어떠한 보안위험이 존재하고 있는지 등의 여부를 체크하고 그 정도를 나타내는 데 있다.

따라서 기업에 있어서 가장 중요한 위험은 '해킹 등 외부의 침입', '내부 정보자산의 무단유출', '정보자산의 절취 후 무단활용' 등이므로 통합 라이프사이클 단계와 그에 속한 보안지표 및 위험지수의 활용, 보안지표 정보의 자동화된 수집과 징후탐지 시스템 활용 등을 포함하여 지표정보수집 → 보안지표 상시측정 → 위험지수의 산출 → 개선활동 → 지표정보수집 등으로 운영되는 사이클 모델을 Fig 6.과 같이 설계하였다.

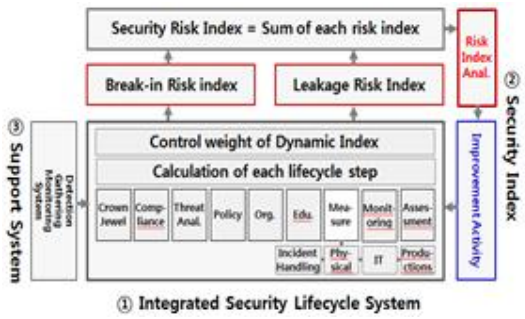


Fig. 6. Model of 'Enterprise Type Realtime Security Management System"

'기업형 상시 보안관리 체계'의 구현단계는
① 보안업무의 라이프사이클 단계를 정의
② 각 라이프사이클 단계별 보안지표를 설정
③ 보안지표 별 '동적지표', '침입위험 지표', '유출위험 지표' 등의 특성을 부여
④ 보안지표 수집, 징후탐지 시스템을 구축
⑤ 시스템에 의한 '상시 모니터링' 프로세스 화
→ 주기적인 종합위험지수 산출 보완.

여기에서 도출된 '종합위험지수'가 '0'일 경우, 완벽한 보안관리 체계로 간주할 수 있지만 '완벽한 보안'이란 불가능 하므로 일정 수치의 위험지수가 나오게 되며 종합 험지수를 역으로 분해하여 영역별로 분석하면 위험을 조기 인식하여 선제대응 할 수 있다.

V. 기업형 상시 보안관리 체계의 검증

5.1 K-ISMS 관리체계와의 비교

제시된 '기업형 상시 보안관리 체계(6) ETR-ISMS)'와 K-ISMS 관리체계를 비교해 보면 K-ISMS는 보안업무의 관리체계 운영여부를 중시한 측면이 있었고, ETR-ISMS는 다음 표와 같이 각 개별 보안영역의 수준을 나타낼 수 있고, 모니터링 영역에서는 실시간 보안수준의 감시가 가능하며, 위험지수에 의한 각 영역의 위험을 조기 인식 가능한 장점을 가지고 있다.

이렇게 '기업형 상시 보안관리 체계'를 활용할 경우,

첫째, '종합위험지수'는 조직의 보안위험 정도를 나타내 줄 수 있으므로 보안관리자, CSO 등도 취약한 부분을 신속히 인지하고 대응책을 수립하게 할 수 있다.

둘째, '동적지표'를 활용함으로서 핵심적 위협요인을 표시할 수 있으므로 선제대응이 가능해 지고,

6) Enterprise type realtime ISMS

Section	ETR-ISMS	K-ISMS	Difference
Goal	– Building Enterprise Type Real time ISMS	– Building Total Security Management System	Real time vs Making Process
Contents	– 9 domains, 160 items Crown Jewel Compliance Threat Analysis Policy Organization Education & P.R. Applying measure Monitoring Check & assessment	– 13 domains, 92items Policy Classification Organization Education Human Contracter Physical Operation Mgnt. Access Crypto. Development security Incident handling Disaster Recovery	ETR. added monitoring domain and eliminate the domains except sec–urity.
Result	– Can identify the security level of each domains	– Can't	ETR can establish the countermeasu–re rapidly
Durab–ility	– Can check the status of security level during certain period	– Check the status of security level at present time	ETR can encourage to keep the high level security
Real–time	– Can check the security operation status at real time using monitoring domain	– Can't	ETR can monitor the security status continuously
Sensi–tivity	– Can recognize the risk of each domains by risk index	– Can recognize the risk after the total check and analysis process	ETR can response early

Fig. 7. Comparison of K-ISMS vs. Enterprise Type RealTime Security Management System

셋째, '모니터링' 활용으로 상시적인 위협요인을 관찰할 수 있으므로 신속한 대응이 가능해 질 수 있을 것이다.

5.2 AHP 방법론에 의한 검증

제안된 '기업형 상시 보안관리 체계'의 배경, 특성의 타당성 여부 검증을 위해 7)AHP(Analytic Hierarchy Process) 방식을 활용하였는데 분석목표를 '보안관리 체계의 핵심특성 중요도 우선순위 결정' 으로 하고 1계층은 운영목적인 '사고예방, 지속적 관리, 전사적 적용' 3개, 2계층은 1계층의 각 영역별 '위협요인 도출' 등 16개 등으로 다음과 같은 AHP모델을 설계하였다.

5.2.1 AHP 계층모델에 대한 설문조사 분석결과

설문조사는 응답내용의 신뢰도 확보를 위해 각 조직의 보안관리 책임자(보안업무 경력 15년 이상) 22명을 대상으로 실시하고 그 결과를 AHP 전문분석 프로그램인 Expert Choice 2000으로 분석하였다.

7) 다기준 의사결정 문제에서 평가기준과 대안을 계층적 구조로 파악하여 최적대안을 선택하는 방법론으로 Thomas Saaty(1980)에 의해 개발

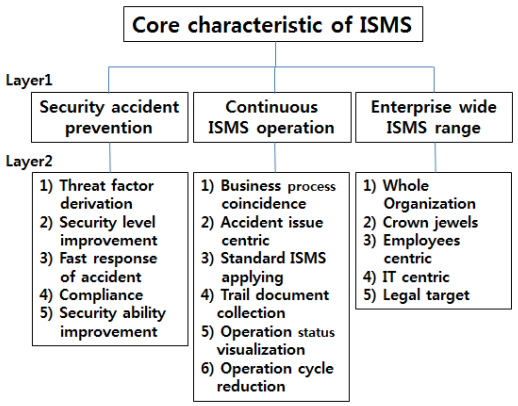


Fig. 8. Layered AHP model to derive the core-characteristic of ISMS

(25명 중 Inconsistency가 0.1이하인 22명 대상)

다음은 Expert Choice 로부터 추출된 전체 16개 요소의 중요도 순위이다.

분석결과, 16개 요소의 중요도 우선순위에서는 핵심자산(8.2), 신속한 사고대응(8.0), 위협요인 도출(7.3) 등으로 나타났는데 이는 '기업형 상시 보안관리 체계'가 추구하는 동적지표의 활용, 위험지수의 산출목표 등과 합치한다는 것을 알 수 있었다. 또한 쌍대비교 분석결과에서도 1계층에서는 '사고예방'(0.648), '지속적 관리'(0.198), '전사적 적용'(0.154)의 순으로 중요도가 결정되었고, 2계층에서도 '사고예방' 분야에 속하는 '신속한 사고대응'(0.214), '위협요인의 도출'(0.157), '법률준

Fig. 9. The Priority result of core characteristic of ISMS from Expert choice 2000

수'(0.101) 등이 중요도 상위에 위치하였고, 상세 결과는 다음 Table 6과 같다.

결론적으로 '기업형 상시 보안관리 체계'의 특성으로 간주한 '핵심자산, 또는 핵심위협의 중점 관리를 위한 동적지표의 설정', '위협요인의 조기인식 및 사고예방을 위한 위험지수의 산출' 등은 이번 AHP 분석 결과에서도 도출되었듯이 보안관리 체계가 가져야 할 핵심 특성으로서의 그 타당성을 검증할 수 있었고, 반면, '기업형 상시 보안관리 체계'에서 제안한 '통합 보안 라이프사이클 체계의 수립'의 요소인 '보안업무 프로세스와의 일치(Business process coincidence)'가 0.044점으로 7위에 위치, 비교적 중요도가 높지 않았던 분석결과는 대상 조직들이

Table 6. Result of Core characteristic of ISMS From Expert Choice 2000

L1.	L2.	Local rank		local/ global		Final rank
Security accident prevention(0 648)	Threat factor derivation	7.3	3	.242	.157	2
	Security level improvement	7.1	4	.150	.097	4
	Fast Response of accident	8.0	2	.331	.214	1
	Compliance	6.8	6	.156	.101	3
	Security ability improvement	6.8	6	.121	.078	5
	Average	7.2				
Continuous ISMS operation(0 198)	Biz. process coincidence	6.7	8	.224	.044	7
	Accident issue centric	6.2	11	.204	.040	8
	Standard ISMS applying	5.9	14	.182	.036	9
	Trail document collection	5.3	16	.122	.024	12
	Operation stat. visualization	6.1	12	.172	.034	10
	Operation cycle reduction	5.5	15	.096	.019	14
	Average	6.0				
Enterprise wide ISMS range(0 154)	Whole organization	6.1	12	.095	.015	16
	Crown jewels	8.2	1	.464	.071	6
	Employees centric	7.0	5	.165	.025	11
	IT centric	6.3	10	.126	.019	15
	Legal target	6.5	9	.150	.023	13
	Average	6.8				

K-ISMS 등 기존의 보안체계 외에 별도의 표준관리 체계를 운영하고 있지 않아 필요성을 느끼지 못한 것으로 보인다.

VI. 적용사례 및 시사점

6.1 적용사례

'기업형 상시 보안관리 체계'가 실제로 기업을 대상으로 적용될 경우, K-ISMS 보안관리 체계의 인증심사 결과, 또는 기업의 자체 관리체계에 대한 측정결과와 어떻게 차별화 될 것인지를 확인해 보기 위해 기존의 관리체계 모델에 반영된 지표의 점검내용을 새로운 관리체계에 대입하여 예상되는 차이를 비교해 보았다.

6.1.1 'A'사의 K-ISMS 인증심사 결과

다음은 2013년 'A'사의 내부 시스템에 대한 K-ISMS 인증심사 결과 일부이다. 개별 통제항목 중에서 결함사항이 몇 개 존재한다는 형태로 표시되어 있어 전체 보안수준 및 위협의 존재, 침입유출 가능성 여부 등에 대해 분명히 나타나 보이지는 않는다. 예를 들면 '위험분석' 영역에서 통제사항 3개 중 1개가 결함사항으로 측정되었는데 그 사유는 '정보자

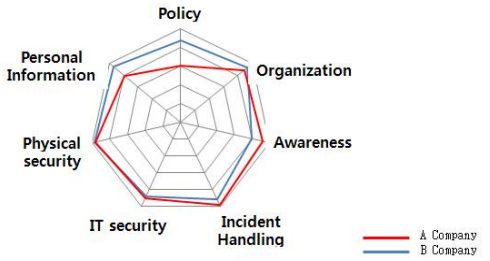
section	Control Activity	Tot	check	Fault	Fault Item Detail
IS Control Steps	1. Policy	2	2	0	-
	2. Organization	2	2	0	-
	3. Threat Analysis	3	3	1	Did not classify Info. Asset
	4. Applying Measure	2	2	0	-
	5. Follow-up Mgnt.	3	3	0	-
Sub-total		12	12	1	
IS Control Areas	1. Policy	6	6	1	Did not share policy
	2. Organization	4	4	1	Didn't have R&R documents
	3. Contract security	3	3	0	Did insufficient check
	4. Classification	3	3	1	Did attach classification mark partially
	5. Education	4	4	0	-
	6. Human Security	5	5	0	-
	7. Physical Security	9	9	0	Found some items that didn't apply SSL
	8. Development Sec.	10	10	1	Didn't keep the standard of coding and develop. process
	9. Crypto. control	2	2	2	Using insufficient Crpto. level
	10. Access Control	14	14	4	Found many violation items about using password
	11. Operation Security	22	22	4	Found insufficient review of firewall and accounts policy
	12. Incident Handling	6	6	0	-
	13. Disaster Recovery	3	3	1	Didn't identify goals of DR.
Sub-total		92	92	15	
Total		104	104	16	

Fig 10. 'A' company's Measurement Result of K-ISMS

산의 비밀분류를 하지 않았다'라는 내용으로서 어떤 정보자산이 분류되지 않았는지 등이 명시되지 않고 있다.

6.1.2 'A'社 자체 보안관리 체계 점검결과

2015년의 자체측정 결과를 보면 각 보안영역별 보안수준 정도를 개략적으로 보여주고 있어 전체 보안수준을 인식할 수는 있고, 또 영역별 미비점을 언급함으로서 보완조치를 할 수 있도록 하고 있지만 침입위험은 어느 정도인지, 유출위험은 얼마나 존재하고 있는지는 파악이 어려워 보인다.



	Tot.	Policy	Org.	Aware-ness	Incident Handling	IT Security	Physical Security	Personal Info.
A Co.	87.3	6.0	13.3	4.6	9.8	36.1	9.6	7.9
B Co.	90.0	8.7	14.0	4.0	9.1	35.2	9.7	9.4

Fig. 11. Measurement Result of Proprietary Security Management System of 'A' Company

6.1.3 '기업형 상시 보안관리 체계' 시범적용 결과

다음은 이러한 'A'사의 현재 보안상황을 본 논문에서 제안한 '기업형 상시 보안관리 체계'를 활용하여 간이 점검을 한 결과이다. 상세한 체크리스트는 A사의 자체 체크리스트를 이용하였다.

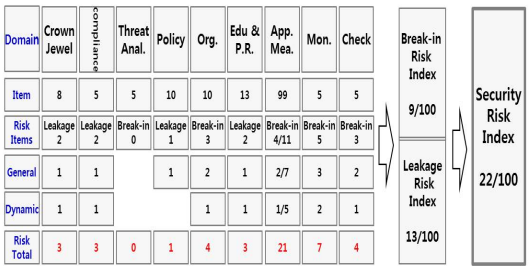


Fig. 12. Calculating Risk Index Value of 'A' Company by Enterprise Type RealTime Security Management System Model.

사전 분류된 보안지표에서 일반지표 G=111, 동적지표 D=49, 침입위험지표 B=120, 유출위험지표 L=40, 침입위험 일반지표 BG=83, 유출위험 일반지표 LG=28, 침입위험 동적지표 BD=37, 유출위험 동적지표 LD=12를 추출하여 다음 식에 의해 라이프사이클 단계별 수준을 측정한 결과, 종합위험지수는 22점으로 파악되었고, 유출위험은 13점, 침입위험은 9점으로서 유출위험이 더 높은 것으로 파악되었다.

$$SRI = \frac{\sum_{i=1}^{G} R(i) + (2 \times \sum_{i=1}^{D} R(i))}{G + 2D} \times 100 = 22$$

$$BRI = \frac{\sum_{i=1}^{BG} R(i) + (2 \times \sum_{i=1}^{BD} R(i))}{BG + 2BD} \times 100 = 9$$

$$LRI = \frac{\sum_{i=1}^{LG} R(i) + (2 \times \sum_{i=1}^{LD} R(i))}{LG + 2LD} \times 100 = 13.$$

다음은 이를 영역별 분포도로 나타낸 결과이다.

즉, 본 연구에서 제안한 '기업형 상시 보안관리 체계' 모델을 A사에 적용한 결과, 각 영역별 위험수준을 잘 알 수 있었고, 위험분포도를 통해 보완해야 할 내용이 나타나 신속한 대응책 수립을 지원할 수 있을 것으로 나타났다. 또 한, 침입위험지수와 유출위험지수를 별도로 산출하여 각 영역별 어떠한 위험이 현재 존재하고 있는지도 잘 알 수 있었다.

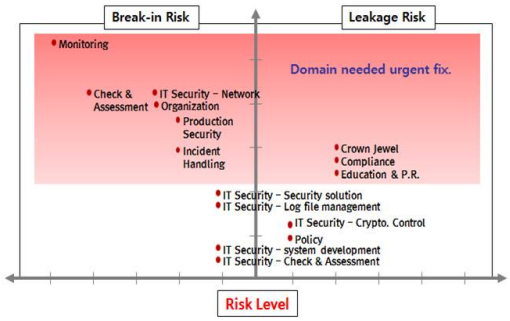


Fig. 13. Representing the Risky part of Security Management Domain of 'A' Company

6.2 시사점

보안관리 체계 별 지향하는 고유의 목적과 목표, 방법론이 있지만 궁극적으로 공통된 목표는 조직의 보안강화로 볼 수 있다. 즉, 보안을 강화하는 과정에

서 기업에서의 '보안관리 방법론'이 가져야 할 핵심적 조건은 본 논문에서도 언급한 바와 같이 상시성, 지속성, 인식성 등의 3가지라고 할 수 있다. 따라서 '기업형 상시 보안관리 체계', 혹은 K-ISMS, 'A'사의 보안지수 관리체계 등의 상호간 장점을 취해서 개선, 보완한다면 보다 더 효율적으로 보안강화 목표를 달성할 수 있을 것이다.

VII. 결 론

최근 기업을 둘러싼 정치, 사회, 경제, 기술적 환경들은 기업으로 하여금, 한 순간 뒤쳐질 경우, 생존 자체를 위협받게 될 정도로 변화하고 있다. 보안 측면에서도 이러한 최근의 환경을 감안한다면 가장 큰 우선순위는 '신속한 대응'일 것이다. 즉, 위협요인을 신속하게 감지하고, 그에 대한 대응책을 수립하여 조기대응 하는 것이다. 본 연구에서는 이러한 '신속한 대응'을 위하여 기업의 보안을 상시적, 지속적으로 유지할 수 있도록 '기업형 상시 보안관리 체계'의 구축을 제안하였다.

제안된 관리체계의 구축에 필요한 사항을 요약하면.

첫째, 조직의 내부 보안상황을 잘 나타내 줄 수 있는 보안지표의 설정이 가장 중요하다. 즉 현재 시점에서 어떤 위험이 있는지를 나타내 줄 수 있고, 개별적이 아닌 전반적인 문제를 도출할 수 있어야 한다. 즉, '서버의 어떤 취약점이 존재하고 있는지'가 아니라 '서버의 취약점이 왜 제거되지 않았는지.'등으로 문제현상이 도출되어야 하며, 보안지표의 내용도 기업의 특성에 따라 달라져야 한다. 즉, 금융회사는 개인정보, 제조기업은 산업기술 등이 중심이 되어야 할 것이다.

둘째, '동적지표'의 설정이다. 한 시점에서의 현상을 체크하는 것만 아니라, 지표 자체가 일정기간 동안의 보안 수준을 충분히 나타낼 수 있도록 설정되어야 하고, 치명적 보안필요 사항을 도출하여 지정하여야 한다. 예를 들면, 악성코드의 내부 확산 시 기업이 치명적 피해를 입게 되므로 점검시점에서 '악성코드 감염 조치여부'가 아니라 과거 조치 이력을 포함한 '악성코드의 조치시간 관리' 등을 동적지표로 설정하여 평소 악성코드 관리 상태를 점검할 수 있어야 한다.

셋째, 지속적인 모니터링에 의해 보안수준이 항상 유지될 수 있도록 관리해야 한다. '일일 보안상황 관리' 등의 주기적 감시활동을 통해 신규 발생하는 위협요인 등이 현재의 보안상태에서 조직의 비즈니스에 어떠한 영향을 끼칠 수 있을 것인지 정보수집 및 분석을 철저하게 실시해야 것이다.

넷째, 이러한 보안관리 체계의 정상적인 운영을 위해서 필요한 시스템화, 또는 자동화가 뒷받침되어야 한다. 갈수록 복잡해지는 경영환경에서 수많은 보안지표들과 체크리스트를 매일매일 수작업으로 점검할 수는 없는 일이다. 따라서 이런 지표들을 자동으로 점검하여 관련자들이 공유하여 신속한 대응 조치가 이루어질 수 있도록 해야 한다.

다섯째, 본 연구에서 제안된 '기업형 상시 보안관리 체계' 가 K-ISMS나 기업 자체적으로 운영중인 관리체계에 비해 뛰어나다는 것이 아니라 각 관리체계 별 특성을 가지고 있고, 조직별 현안 및 특성에 따라 이러한 관리체계의 내용을 참조하여 적합한 관리체계를 구축해야 한다. 예를 들면 K-ISMS는 보안의 지속적인 관리를 목표로 하고, 기업의 자체 관리체계는 우열을 가려서 보안수준 제고를 촉진하기 위한 것이며, '기업형 상시 보안관리 체계'는 조직의 보안 위험을 빨리 찾아내어 신속대응 하기 위한 것이다.

마지막으로 본 내용이 많은 기업의 보안담당자들이 효율적인 보안체계를 구축하는데 도움이 되었으면 한다.

References

[1] PCworld, "*Sony Sued Over PSN Data Breach, Failure to Disclose*", http://www.pcworld.com/article/226478/sony_sued_over_psn_data_breach_failure_to_disclose.html, Apr 27, 2011

[2] Seung-Ju Kim. "*Have to lead the 'Creative Security' against industry*", http://www.dt.co.kr/contents.htm?article_no=2011080902012251697035, Aug 8, 2011

[3] KQA, "ISO/IEC 27001:2013 Framework overview", http://kqa.co.kr/main.php, Jun 15, 2017

[4] KISA, "2017 ISMS certification system briefing session", https://isms.kisa.or.kr/main/isms/notice/?boardId=bbs_0000000000000001&mode=view&cntId=48&

category=%EC%9E%90%EB%A3%8C&pageIdx=1, Apr 27, 2017

〔5〕 KISA, "Detail check list of ISMS certification", https://isms.kisa.or.kr/main/isms/notice/?boardId=bbs_0000000000000001&mode=view&cntId=36&category=%EC%9E%90%EB%A3%8C&pageIdx=2, May 15, 2013

〔6〕 Haider Abbas, Christer Magnusson, Louise Yngstrom and Ahmed Hemani, "*Addressing dynamic issues in information security management*", Information Management & Computer Security. 19, pp. 4, Jan. 2011

〔7〕 BCS, "*Why ISO27001 is not enough?*", http://www.bcs.org/content/ConWebDoc/26594, IT Research Lab, pp. 1-2, 2009

〔8〕 Hee-Myung Lee and Jong-In Lim, "*A Study on the Development of Corporate Information Security Level Assessment Models*", Journal of the Korean Institute of Information Security and Cryptology, pp. 165-169, Jul. 2008

〔9〕 Shin-beom Kang, "*A Study on the Effective Countermeasures for Preventing Computer Security Incident*", pp. 71-82, Feb. 2012

〔10〕 Sang-Eun Kwon, KAIST, "*Research of Information Security Management Model for Real-Time Security Level Measurement*", KOASAS(KAIST open access self archving system), pp.2, 2013

〔11〕 Yu-Chan Ko, "*A Study on an Improvement of Information Security Management System (ISMS) Scheme- Flexible Application of Control Items*", Research Information Sharing Service(RISS), pp. 42, Dec, 2013

〔12〕 Kyung-Ho Lee, "*Method and Apparatus for Measurement of Information-Security-Controlling Status*", Patent No. 10-1616989-0000, pp. 5-6, March, 2016

〔13〕 Symantec, "*Internet Security Threat Report*", Volume 21, pp. 2, 2016

〔14〕 ETnews, "*1 Billion PCs At Risk As Windows Error Reporting Sends Reports In Clear*(Original Title)", http://www.etnews.com/201401020348, Jan 2, 2014

〔15〕 Dailysecu, "*Possibility of Anonymous FTP attack for Domestic NAS servers.*", http://www.dailysecu.com/?mod=news&act=articleView&idxno=5930, Dec 17, 2013

〔16〕 Boannews, "*Exposure of domestic gas measurement system information at Shodan*", http://m.boannews.com/html/detail.html?idx=49636, Feb 17, 2016

〔17〕 ETnews, "*The warning of Semiconductor hacking threats. Industries preparing countease.*", http://www.etnews.com/201401160301, Jan 16, 2014

〔18〕 Yonhapnews, "*'Hacking suspicion' Chinese PC, Withdraw from British intelligence agency*", http://www.yonhapnews.co.kr/bulletin/2013/07/30/0200000000AKR20130730184900085.HTML, Jul 30, 2013

〔19〕 Spiegel Online, "*Documents Reveal Top NSA Hacking Unit*", http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html, Dec 29, 2013

〔20〕 Eun-Sung Kang, "*The CISO Story of Eunsung Kang*", i-News24 Opinion column, http://opinion.inews24.com/php/news_view.php?g_serial=835179&g_menu=042137, Jul 11, 2014

〔21〕 Eun-Sung Kang, "The Information Security that CxOs have to know", Hanbit Media, Seoul, 296, 2015

〔22〕 Il-Jun Moon(CEO of Bitscan Company), "*Is the ISMS certification company safe from hacking?*", http://www.dailysecu.com/?mod=news&act=articleView&idxno=3677, Jan 23, 2013

〔23〕 NIST. "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and*

Organizations." Special Publication 800-137: https://www.nist.gov. Sep 2011

〔24〕 Chae-Ho Lim(The Former Professor of KAIST University), "*The need of Total ISCM strategy for continuous security monitoring*", http://www.boannews.com/media/view.asp?idx=49305, Jan 25, 2016

〔25〕 The KPI Institute, *"New SmartKPIs.com Report Ranks The Top IT Security KPIs of 2011- 2012"*, https://news.kpiinstitute.org/new-smartkpis-com-report-ranks-the-top-it-security-kpis-of-2011-2012/, May 20, 2013

〔26〕 Jung-Sik Ryu(CEO of 'In Future' Company), "*Give up the unconditional trust about KPI*", http://www.infuture.kr/1444, Apr 14, 2014

〔27〕 KISA, *"A Study on National Information Security Evaluation Indices and their Internationalization"*, R&D Report, 06-1. 2006

〔28〕 KISA, *"Encryption action guide of the Privacy Informations"*, Jan, 2017

〔29〕 Yun-hyun Kim, Tae-Seung Lee(KISA), *"Main Issues and the weakness analysis of Internat Cookies"*, INTERNET & SECURITY FOCUS, pp. 84-85, Aug, 2014

〔30〕 Russia Focus, *"Russia〈Personal Information Act〉Amendment Law Enacted in September. -Russian personal information have to save at the domestic servers"*, https://russiafocus.co.kr/society/2015/04/10/9_46959, Apr 10, 2015

〔31〕 ITworld,*''Europe approves new data protection law-European Parliament gives massive support to stronger data protection rules"*, http://www.itworld.com/article/2831822/it-management/europe-approves-new-data-protection-law.html, Mar 12, 2014

〔32〕 Juniper Networks, "*The Economics of Defence", from RAND Corporation's "Defender's Dilemma: Charting a Course Toward Cybersecurity*", pp. 9, Aug,. 2015

〔33〕 CONCERT, "*Security Consumer Report - Information Security Performance Indicator*", CONCERT Homepage, pp. 4-6, Nov. 2013

〔34〕 KISA, *"An Analysis of economic effectiveness on ISMS Certification"*, Internet & Security issue, pp. 30, Mar. 2010

〔35〕 Sang-su Jang, *"The Effects of the Operation of an Information Security Management System on the Performance of Information Security"*, Journal of the KIISE, Information Networking, Vol. 40(1), pp. 58-69, Feb. 2013

〈저자소개〉

노 시 영 (Shi-Yeong Noh) 종신회원
1983년 8월: 동아대학교 수학과 학사
2016년 1월: 삼성SDS 고문
2017년: 고려대학교 정보보호대학원
〈관심분야〉 기업보안, 보안정책, Forensic

임 종 인 (Jong-In Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사
2000년 8월: 고려대학교 정보보호대학원 원장
2005년 7월: 대통령 자문 전자정부 특별위원
2012년 6월: 고려대학교 정보보호대학원 사이버국방연구센터장
2015년 1월: 대통령 비서실 안보특별보좌관
〈관심분야〉 정보보호, 전자공학, 통신공학