산업보안 경영시스템 구축을 위한 자산 및 위험평가에 관한 연구

고 준 철* · 김 태 수* · 주 용 마* · 김 우 현* · 강 경 식*
*명지대학교 산업경영공학과

A Study of Asset and Risk Assessment for Established of Industrial Security Management System

Joon-Cheol Koh* · Tae-Soo Kim* · Yong-Ma Joo* · Woo-Hyun Kim* · Kyung-Sik Kang*
*Department of Industrial Engineering, Graduate School, University of Myongji

Abstract

The purpose of this study is, by recognizing that recently, as crimes using information and various adverse-effect phenomena such as hacking and virus occur frequently with rapid development of information network such as Internet in every field of industry, the range of security is widening to the field of industrial areas for preventing the leaking of industrial technology and protecting that technology as well as information security only limited to IT area, and by establishing common concept about industrial security through education on the industrial security at the point of increasing importance of industrial security, to prepare the base of comprehensive risk management system for protecting company's assets (physical factor, technical factor and managerial factor) safely from the random threats or attacks inside and outside the company through assessment of important assets of the company, evaluation of threats and weak points, and risk assessment by building industrial security management system in order to protect company's information assets and resources which are connected to the existence of the company safely from the threats or attacks from inside or outside the company and to spread stable business activities.

Keywords : Industrial security Management System, Asset and resources, Risk assessment

1. 서 론

오늘날 보안(Security)은 전 영역에서 화두가 되고 있으며, 보안의 영역이 정보보안이라는 한정적으로 이해하는 부분이 많았으나 최근 모든 산업분야에서 인터넷 등 정보통신망의 급속한 발전과 함께 해킹, 바이러스 등 정보범죄와 정보화에 따르는 각종 역기능 현상이 많이 발생하면서 IT에 국한된 정보보안만이 아니라 산업기술 유출방지를 위한 산업보안으로 확산되고 있다. 산업보안의 중요성이 증대되고 있는 시점에서 산업보안 교육을 통한 산업보안에 대한 공통적인 개념을 정립하고, 기업의 생존과 직결되는 기업 중요 자산과 자원을 내·외부의 위협이나 침입으로부터 안전하게 예방하고 안정적인 경영활동을 전개할 수 있도록 산업보안 경영 시스템 체계를 갖추어 내실화 해 가는 것이 무엇보다 중요한 요소다.

지식정보화 시대에서는 모든 기업 활동과 사회생활에서 정보 자체가 주요한 원천이 된다. 그러나, 정보를 취급하는 과정에서 오는 취약성으로 인하여 정보에 대한 무단 유출 및 파괴, 변조 등과 같은 위협이나 공격이 자행되고 있으며, 또한 인가받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전한 정보의 유통 등과 같은 피해가 증가하고 있는 것이 사실이다.

† 본 논문은 명지대학교 안전경영연구소 협력에 의해 이루어진 논문임.
† 교신저자: 고준철, 경기도 안양시 만안구 안양6동 호정타워 212호
M · P: 010-6363-4137, E-mail: tobe0515@empal.com
2010년 10월 19일 접수; 2010년 12월 4일 수정본 접수; 2010년 12월 6일 게재확정

이에 대한 산업기술 유출 사례를 살펴보면 2008년 한 해 동안만 42건에 예상 피해액 79조 8,000억원에 이르며, 분야별로는 조선 분야 핵심기술 기도(32조원), PDP 핵심기술 해오 유출(3년간 약 1조 3천억원), 재활용 신기술 해외 유출 기도(1조원), 디지털 방송분야 셋톱박스 해외 유출 기도(약1조5천억), 이동통신 분야 '모바일 멀티미디어 플랫폼 칩' 기술 해외 유출 기도(2.3조원) 등으로 전 산업 분야로 확산되어 어떤 산업 분야에서도 안심할 수 없는 것이다(출처 : 국가정보원 산업기밀보호센터 '08).

지금까지 기업이나 조직단체가 정보보안에 대한 중요성을 인식하면서도 IT기반의 정보보안에 대해서는 철저하게 대응하면서 산업보안의 중요성에 대해서는 간과하는 경향이 많았다.

산업보안의 개념은 산업 활동에 유용한 기술이나 경영활동에 필요한 정보와 기술을 각종 침해 행위로부터 안전하게 보호, 관리하기 위한 대책과 활동으로 정의하고 있다.

최근에는 국내에서도 크고 작은 보안사고가 급속하게 증가하는 실정이고, 산업보안에 대한 다양한 기술과 인프라를 구축하고 통제하고 있지만 가장 중요한 것은 산업보안에 대한 정책을 수립하고, 조직 구성원들에게 산업보안의 중요성을 인식할 수 있는 교육훈련이 강화되어야 함은 조직원의 사소한 보안 위반이 기업 경영전략 수립 및 기술보호에 큰 영향을 초래하기 때문이다. 따라서, 본 연구에서는 지금까지 정보보안에 대한 사고를 산업보안 측면에서 산업 기술보호를 위해 산업보안 경영시스템을 구축하고 실행함에 있어서 자산평가, 위험분석 및 위험평가 구조(Framework)를 정립하여 산업보안의 체계적인 관리와 모니터링을 통해 기업의 핵심 자산인 산업정보 및 기술유출 방지와 보호에 대처할 수 있는 기반을 제공하고자 한다.

2. 이론적 고찰

2.1 산업보안의 개념

기업에서 정보보안이라 함은 한 기업이 가진 중요정보 혹은 기업간의 상거래에서 발생하는 거래정보의 '기밀성(Confidentiality)'과 '무결성(Integrity)', 그리고 이에 사용되는 정보시스템 및 데이터의 '가용성(Availability)'을 보장해주는 것을 말한다. 산업보안이란 산업 활동에 유용한 기술이나 경영에 필요한 정보와 기술을 각종 침해 행위로부터 안전하게 보호·관리하기 위한 대책과 활동으로 정의한다.

기업 경영활동의 중요한 정보인 인사/노무, 재무/회계, 구매 및 생산정보, 각종 통계 및 사업전략이나 계획 정보가 인터넷으로 옮겨지고 실시간으로 의사결정을 해야 하는 기업문화가 정착되면서 산업보안이 가지는 의미는 더욱 중요해지고 있다.

산업보안에 대한 주요 환경변화 요인이 목적과 수단, 대상에 따라 변하고 있는데 목적이 과거 냉전시대에는 개인이나 기업보다 국가 경제 발전이나 군사 목적으로 정보를 수집하였다면 현재는 탈 냉전시대로 기업 경쟁력 확보와 첨단 산업기술을 수집하는 것으로 변했고, 수단으로는 아날로그 시대에 문서, 노하우 전수 등 제한적 유출수단에서 디지털 시대에는 대용량 매체를 이용하여 정보 유출이 용이해졌다는 것이다. 또한 대상은 기술추격 시대에서는 시설, 장비 제품정보가 주류를 이루었다면 기술혁신 시대에는 기술인력, 산업기술 유출이 그 대상이 되고 있다.

1) 산업보안 대책

산업보안에서 기밀성의 유지를 통해 중요한 정보자산이 외부에 노출되지 않으며, 무결성의 확보를 통해 데이터의 객관성(또는 사실성)이 보장되고, 가용성을 통해 언제든지 요구하는 결과를 산출 해 사용할 수 있는 환경을 지속적으로 제공하기 때문에 정보보안의 3요소인 '기밀성', '무결성', '가용성'은 산업보안에서도 필수적인 요소이다.

그렇다면, 무엇으로부터 무엇을 보호해야 할 것인가?

산업보안은 재난과 실수 및 부정한 조작으로부터 기업이 가진 중요 정보를 비롯한 시스템과 서비스를 보호하여 보안사고의 가능성과 영향을 최소화하는 것이다.

지금까지 공개적으로 알려진 산업보안의 취약점으로 인해 발생된 기술유출 사례를 보면서 산업보안 대책의 필요성을 재인식하고자 한다.

2006년 4월 P사 연구실장의 전보인사에 불만을 품고 와이브로드 핵심기술, 노트북, HDD, E-Mail을 이용하여 빼돌린 기술을 업그레이드 후 미국 IT업체에 매각을 기도한 사건과 '07년 1월 중국 정부 합작 선박설계 전문회사 'M사' 부사장의 전직으로 벌크선 설계용역 수주(중국)하여 빼돌린 D사 설계도면을 전달하여 설계에 참고하고 인도, 이란 등 조선소 건설에 참여한 후 D사 유출 자료를 소지하고 중국으로 출국시 검거된 사례를 보면 산업기술 유출방지를 위해 체계적인 산업보안 대책 수립이 필요하다.

2) 산업보안 기술보호 정책

산업보안 정책은 기업 내에서 계획적, 우발적 모든 위협으로부터 자산을 보호하고 산업보안 업무를 관리하기 위한 수단이다.

일반적으로 정보보안 정책의 유형은 프로그램 정책(Program policy), 이슈 지향적인 정책(Issue-specific policy), 시스템 지향적인 정책(System-specific policy)로 구분하고 있으며, 산업기술보호 정책은 기업의 정상적인 경영활동은 최대한 보장하고, 국가 핵심기술 지정 및 체계적인 관리, 산업 기술 불법 유출 대응 체계 구축, 산업기술 보호 역량 강화를 위한 산업기술 보호기반 구축지원, 산업 보안 의식 제고를 위한 교육·홍보를 강화하는 추진체계를 확립하는 것이다.

2.2 산업기술보호 추진체계

1) 국가 핵심기술의 개념

국내외 시장에서 차지하는 기술적 경제적 가치가 높거나 관련 산업의 성장 잠재력이 높아, 해외 유출시 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술로 정의한다.

국가 핵심기술의 보호를 위한 범정부적 대응을 위해 『산업기술의 유출방지 및 보호에 관한 법률』을 제정(지식경제부(구 산업자원부), 07.3월)하고, 국가 핵심기술을 분야별로 지정하여 관리하고 있다.

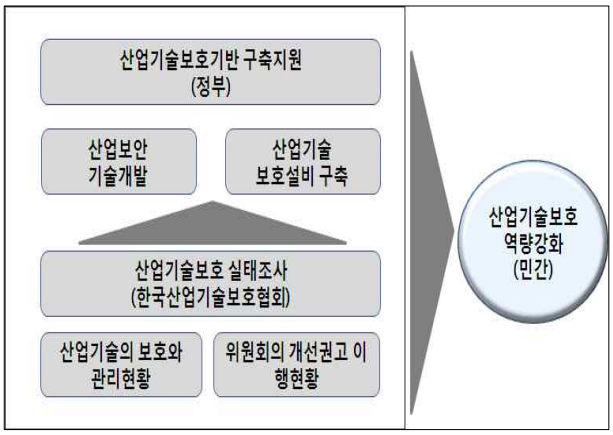
2) 산업기술보호 기반 구축

산업기술 보호 기반 구축을 위해 산업기술 보호와 관리 현황과 위원회의 개선 권고 이행 현황에 대한 산업기술보호 실태조사를 실시하여 업종별, 분야별 산업보안 기술 개발 부문과 산업기술 보호설비 구축, 산업기술 보호 지역 혁신센터 운영지원 등 정부차원의 지원이 이루어지고 있다. 산업보안기술 개발, 산업기술보호 설비 구축 등의 지원을 통한 민간의 산업기술보호 역량 강화 측면에서 산업기술보호기반 구축 지원체계를 정립하고 범 국가 차원에서 지원을 하고 있다.

<표 2.1> 국가 핵심기술 지정현황 : 7개 분야 40개 기술

전기전자	자동차	철강	조선	원자력	정보통신	우주
4	8	6	7	4	6	5

(출처: 산업기술의 유출방지 및 보호에 관한 법률;2009.4 지식경제부)



<그림 1> 산업기술보호기반 구축지원 체계

3) 산업기술보호 교육·홍보

산업보안 의식제고를 위해 관계중앙행정기관과 한국산업기술보호협회(KAITS)가 연계하여 산업기술보호 교육과정 개발 및 교육훈련을 실시하며, 산업기술 보호를 위한 홍보활동을 강화하고 있다.

산업보안 의식 제고를 위한 산업기술 보호 교육 및 홍보 활성화 추진 과제로 매년도 교육과정, 교육일정, 전문강사 인력 활용 등에 대한 교육훈련 계획, 산업보안 관련 국내외 최신 정보수집 제공 등에 관한 홍보계획 을 수립하고 다양한 전문 교육과정을 개발하고 운영하고 있다. 이와 관련한 사례로 산업보안 전문 진단사 및 산업보안관리사 양성 과정을 개설하여 운영 중이며, 대상기관 임직원을 대상으로 월 1회 산업기술보호 교육과정을 개설하여 제공하고 있다(이와 관련한 구체적인 사항은 해당기관 홈페이지(www.kaits.or.kr 참조).

2.3 기술 유출 및 침해 예방법

산업기술 유출 방지 및 보호에 관한 법률(법률 제9368호,2009.1.30 일부개정)에 지식경제부 장관은 산업기술의 유출방지 및 보호에 관한 기본계획을 수립하고 시행토록 법적으로 제시하고 관리가 되고 있지만 산업기술 유출별 침해 예방 방법은 다음과 같이 기업의 보유 자산에 대한 분류, 자산에 대한 위험평가, 각종 규정 수립, 산업보안 조직구성, 조직관리(내부, 제3자 포함)와 외부의 불법이나 악의적인 침입방지, 정보시스템 관리, 보조기억매체관리, 보안사고 복구계획, 산업기술 보호 문화를 정착하는 것이다.

1) 보유 자산에 대한 분류

기업이 보유하고 있는 자산을 기준에 따라 분류하고, 자산의 유형, 속성 등을 고려하여 분류기준을 수립한다.

일반적으로 자산유형에 따라 시스템 자산, 네트워크 자산, 응용시스템 자산, PC 및 기타자산, 자료 및 정보, 물리적 자산, 인적자원 등으로 분류한다.

2) 자산의 위험도출 및 대책

정보자산의 중요도 평가는 정보자산의 기밀성, 무결성, 가용성 관점에서 손상되었을 경우 발생할 수 있는 예상 피해 정도를 고려하여 자산의 보호등급을 부여하며, 보호등급이 높을수록 보안수준을 요구한다.

위협 및 취약점 식별은 평가대상 자산에 대해 기업에서 발생할 수 있는 사고나 우려사항 항목을 설정하고 발생 가능성 유무를 확인 한다.

3) 기술유출 방지 규정 수립

산업기술 유출방지를 위해 기업의 규모와 특성에 따라 규정을 수립하여야 한다. 수립될 규정에 포함되어야 할 사항은 보유자산 분류 및 통제, 산업기술 보호조직 구성 및 운영, 인력관리, 침입방지, 정보시스템 관리, 사고의 대응 및 복구, 산업기술보호 문화정착 등이 정의되어야 한다.

4) 산업기술 보호조직 구성 및 운영

정보보안 이나 산업보안 측면에서 가장 통제하기 어려운 부분이 인력에 대한 사항이며 산업기술 보호를 위해 산업기술보호 조직을 구성하여 운영하여야 한다.

최고 경영자의 강력한 의지표명과 산업기술 관리 위원회, 산업기술 총괄 책임자(CSO), 각 부문별 책임자 및 담당자를 구성하여 역할과 책임을 명확하게 정의하고,체계적으로 운영하여야 한다.

<표 3.1> 자산 식별 및 분류

자산식별	설명	해당 예시
정보/데이터	유형, 무형의 정보 또는 데이터	고객, 인사, 회계 정보
하드웨어	시스템 하드웨어	서버, 네트워크, PC
소프트웨어	패키지 소프트웨어, 응용소프트웨어	OS, 패키지, 개발응용SW
서류	문서 형태의 출력물	계약서, 기획서 등
물리적 자산	시스템 하드웨어를 제외한 물리적 자산	UPS, CCTV, 항습기 등
인적자산	정보시스템 사용, 운영 및 관리를 담당하는 인력, 제3자 등	조직원, 퇴사자, 제3자
기타	무형의 이미지	회사평판, 브랜드 등

5) 사고 대응 및 복구 계획

사고 대응 및 복구를 위한 계획을 수립함에 있어 기술 유출방지를 위해 지켜야 할 사항을 포함한 침해 예방 계획 수립과 침해사항 가정, 부서 및 인력별 조치사항을 포함하는 사고 조치계획 수립, 업무 정상화를 위한 내용을 규정하는 복구계획을 수립하여야 한다.

3. 자산 가치 평가

3.1 자산의 정의

광의의 개념에서 살펴보면 기업경영에 필요한 모든 것이 자산이라고 할 수 있지만 기업이 보유한 가치를 지닌 것을 말하며, 산업보안시스템 구축시 자산에 대한 정의에 따라 자산에는 정보자산, 소프트웨어 자산, 물리적 자산, 사람, 서비스, 회사 이미지 및 명성 등이 있다.

3.2 자산 식별

자산은 기업 규모나 사업 특성에 따라 다양하고, 그 수나 종류가 다양하기 때문에 산업기술 보호 세부규정에서 정의한 보유 산업기술의 분류와 ISO 27001 국제표준 규격(2005)의 자산관리 및 분류기준을 기반으로 다음과 같이 자산을 비용이나 규모에 따라 크게 식별한다.

기업의 자산 관리자는 해당 업무 사업장에서 관리해야 할 자산의 범위를 정의하고, 관리 범위 내에 존재하는 자산의 신규 도입/획득, 이동, 변경, 폐기 등에 따른 변경 관리를 지속적으로 이행한다.

3.3 자산 분류체계

자산이 적절한 수준의 보호를 받을 것을 목적으로 분류되어야 하며, 자산의 가치평가에 따라 취급 및 분류되어야 하고, 추가적인 보호와 강화된 처리를 요구할 수 있어야 한다.

자산분류는 자산의 중요성에 따라 기밀성(C), 무결성(I), 가용성(A)을 기반으로 자산 분류 등급에 따라 분류 한다.

자산 분류 및 등급체계는 자산의 기밀성, 무결성, 가용성에 따라 중요도를 평가하고 등급 기준에 따라 적절하게 분류 표시 및 취급 및 보안상의 관리와 통제를 강화하여야 하며, 기업의 산업보안 정책에 따라 자산의 식별 및 분류체계가 재 정립 될 수 있다.

또한 산업보안 시스템이 도입되고 실행을 통해 중요한 자산의 가치가 높아지면 해당 자산의 취약점 및 위

<표 3.2> 자산 중요도 평가를 위한 분류 기준

구분	하	중	상
기밀성 (C)	자산이 외부에 공개되어도 무방한 정도를 의미	자산이 유출되는 경우에 업무 수행에 장애를 주거나 개인 신상에 영향을 줄 수 있는 정도를 의미	자산이 유출되는 경우에 업무 수행에 중대한 장애를 주거나 개인 신상에 심각한 영향을 줄 수 있는 정도를 의미
무결성 (I)	자산이 변조되어도 업무 장애 우려나 개인 신상에 영향을 거의 주지 않을 정도를 의미	자산이 변조되는 경우 업무 수행에 장애를 주거나 개인 신상에 영향을 줄 수 있는 정도를 의미	자산이 변조되는 경우에 업무 수행에 중대한 장애를 주거나 개인 신상에 심각한 영향을 줄 수 있는 정도를 의미
가용성 (A)	자산이 제공되지 않는 경우에도 업무에 장애를 끼칠 우려나 개인 신상에 영향을 거의 주지 않을 정도를 의미	자산이 제공되지 않는 경우 업무 수행에 장애를 주거나 개인 신상에 영향을 줄 수 있는 정도를 의미	자산이 제공되지 않는 경우 업무 수행에 중대한 장애를 주거나 개인 신상에 심각한 영향을 줄 수 있는 정도를 의미

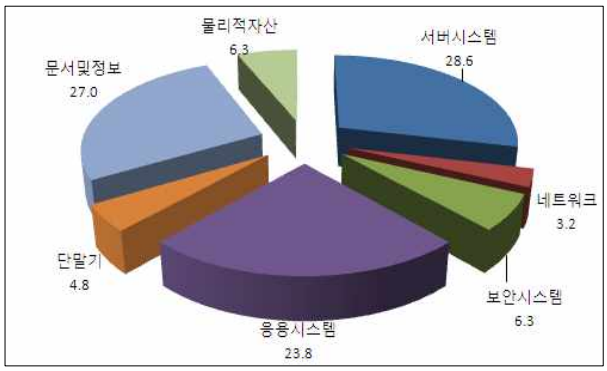
험도를 재 평가하여 지속적으로 보안 수준을 제고하는 노력을 하여야 한다.

자산의 분류 및 등급평가 체계는 ISO 27001국제표준(2005)의 정보분류 기준 정의와 한국산업기술보호협회(KAITS)에서 제공한 산업보안진단 전문가 양성과정의 산업보완 위험분석 및 위험평가 기준체계를 인용하여 해당 컨설팅 중소기업을 대상으로 다음과 같이 정의하고 분류 등급체계에 따라 자산의 가차를 정의한다.

상기의 자산 식별 및 분류체계에 따라 산업현장에서 직접 자산의 가치평가를 실시한 사례를 살펴보기로 한다.

먼저 한 기업의 자산 식별 및 분류 결과를 살펴보면 다음과 같이 하드웨어(서버시스템, 네트워크시스템, 보안시스템, 단말기), 소프트웨어(응용소프트웨어, 상용 소프트웨어), 정보/서류, 인력, 물리적 자산(CCTV, 출입통제시스템 등)으로 분류되었으며, 인력부분에 대한 구체적인 가치평가는 생략하였다.

<그림. 2>자산분류 등급별 가치평가 결과는 <표 3.3> 자산 중요도 평가를 위한 등급평가 기초자료에 의해 평가된 결과이다.



<그림. 2> 자산 분류 등급별 가치평가 결과

<표 3.3> 자산 중요도 평가를 위한 등급평가 사례

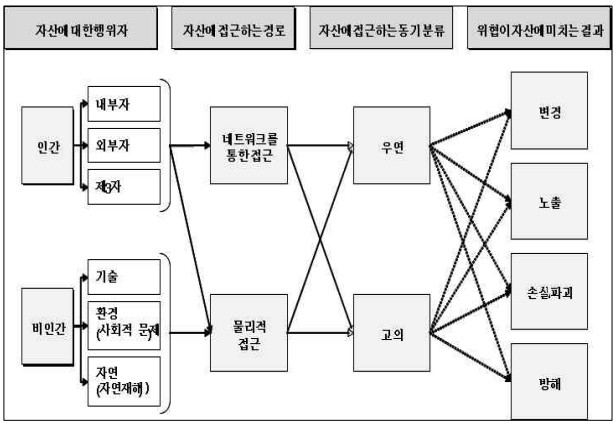
정보자산분류	가등급	나등급	다등급	계	비율
서버시스템	1	7	10	18	28.6
네트워크시스템	0	0	2	2	3.2
보안시스템	0	1	3	4	6.3
응용시스템	8	3	4	15	23.8
상용소프트웨어					
단말기			3	3	4.8
문서 및 정보	17			17	27.0
인적 자산					
물리적 자산			4	4	6.3
[계]	26	11	26	63	100.0

4. 위험평가 및 관리

4.1 위협 및 취약점 평가

본 연구에서는 산업보안 시스템 구축에 따른 자산의 식별과 중요도 평가에 따라 자산의 위험평가 체계를 수립하고 기업이 중요하게 관리되어야 하는 모든 자산을 체계적으로 관리하고 통제하는 구조를 정립하고자 함이며, 이에 따른 제반 평가 절차는 실제 국내 정보통신 제품을 연구개발, 생산 및 현장에 설치하고 유지보수 하는 중소기업체를 모델로 하여 제시한다.

위험평가 및 관리를 위해서는 우선 자산의 식별 및 중요도 평가가 실시되어야 하며, 이에 따라 자산의 위협 및 취약점 평가가 실시되어야 하고, 이를 기반으로 위험평가와 산업보안 경영시스템 체계의 수준이 지속적으로 향상되어야 한다.



<그림. 3> 위협의 종류와 자산에 미치는 결과

4.2 위협 및 취약점 평가 절차

위협(Threat)이란 '원치 않는 사건을 야기하여 회사의 자산에 손실을 줄 수 있는 잠재성을 가지고 있는 것'을 의미하며, 웜/바이러스, 해킹, 소프트웨어의 장애 등이 해당된다.

취약점(Vulnerability)이란 '정보시스템이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인사, 시스템, 장비, 소프트웨어 등의 약점'을 의미하며 정보보안경영시스템(ISMS) 구축 및 실행을 위해 국제표준에서 요구하는 ISO 27001 의 133개 통제항목을 기반으로 평가를 실시할 수 있다.

우선, 위협에 대한 종류와 위협이 자산에 미치는 결과에 대한 흐름을 살펴보면 다음과 같은 종류와 절차에 따른다.

자산에 대한 취약점 평가절차는 1. '자산별 취약점평가 체크리스트'를 구축하여 실시하며, 각 항목에 대하여 관련된 취약점이 존재하지 않을 경우 Y(Yes), 취약점이 부분적으로 존재할 경우 P(Partial), 취약점이 존재할 경우 N(No), 해당 사항이 없거나 관련된 내용이 존재하지 않을 경우 N/A로써 표시하고, 각 항목에 대한 현황을 기록하여 평가한다. 2. 관리적, 물리적 보안 영역에 대한 취약점 평가는 ISO 27001의 보안통제 요구사항 이행여부를 점검하는 방식으로 진행한다. 3. 자산별로 파악된 취약점 평가 결과를 모두 취합하여, '취약점 평가 보고서'를 작성한다.

취약점 평가를 위해서는 취약점 등급기준 설정과 기준에 따라 점수화를 실시하고, 위협 및 취약점 등급에 따라 위험평가에 대응하여야 한다.

취약점 평가를 위해 평가기준은 다음과 같이 정의한다.

ISO 27001(2005) 보안통제 요구사항에 의한 관리적, 물리적 보안 영역의 취약점 평가는 취약점 평가 절차에서 정의한 바와 같이 133개 요소별 취약점 평가를 실시하고 이에 따른 점수화를 통해 위험평가시 기밀성, 무결성, 가용성 측면에서 종합적으로 평가를 실시한다.

취약점을 보안통제 요구사항에 따라 예시로 분류해 보면1.관리적 관점의 분류는 운영적 취약점, 정보보안 관리의 취약점, 인적 취약점, 보안사고 대책관리 등으로 분류 2. 기술적 관점의 분류는 컴퓨터 및 통신관련 취약점, 정보보안시스템 관련 취약점, 시스템 개발관련 취약점 등으로 분류 3. 물리적 관점의 분류는 시설 및 물리적 관점의 취약점, 환경적 취약점으로 분류할 수 있다.

4.3 위험평가(Risk Assessment)

위험(Risk)은 '위협이 취약성을 이용하여 발생하고 그로 인해 자산이 손상을 입게 될 잠재적 가능성'을 의미하며 자산가치 평가, 위협 가능성, 취약점 정도 등이 평가되어야 한다.

4.3.1 위험평가 준비

위험평가를 위한 사전 준비 작업으로 정보 자산 분류 및 자산 가치에 대한 중요도 평가가 실시되어야 하며 이와 함께 조직 및 정보자산의 Gap분석도 중요한 요소이다.

또한, 산업보안 관리체계와 정보자산을 기반으로 위험평가 대상 및 범위가 정의되어야 한다.

위험평가를 위한 사전 체크리스트 준비, 위험평가 Sheet 등이 마련되어야 한다.

<표 4.1> 취약점 평가를 위한 등급기준

취약점 등급	취약점 정도	주요설명
VH	4	보안통제가 없거나 거의 이루어 지지 않고 있어 매우 취약한 상태
H	3	기초적인 보안통제는 실행중인 상태이나 대부분 개선이 필요하고 지속적인 노력과 주기적인 점검이 필요
L	2	기초적인 보안통제는 실행 중인 상태이나 일부분 개선이 필요하고 지속적인 노력과 주기적인 점검이 필요
VL	1	보안통제가 구현되어 실행되고 있으며 매우 양호

<표 4.2> ISO 27001 보안통제항목별 취약점 평가 사례

ISO 27001 통제항목		중요도	진단결과	현재수준 (백분율)	취약점수준	등급
A.5	보안정책					
A.5.1	정보보안 정책					
A.5.1.1	정보보안 정책문서	상	X	0.00	100.00	4
A.5.1.2	정보보안정책의 검토	중	X	0.00	100.00	4
A.6	정보보안 조직					
A.6.1	내부조직					
A.6.1.1	정보보안에 대한 경영의지	상	X	0.00	100.00	4
A.6.1.2	정보보안 협력관계	상	X	0.00	100.00	4
A.6.1.3	정보보안 책임의 정의	상	X	0.00	100.00	4
A.6.1.4	정보처리장비에 대한 승인체계	상	X	0.00	100.00	4
A.6.1.5	기밀유지 협약	상	O	13.04	86.96	4
A.6.1.6	국가기관과의 협력체계	중	X	0.00	100.00	4
A.6.1.7	이해관계/전문가 조직간의 협력	상	X	0.00	100.00	4
A.6.1.8	정보보안의 독립적인 검토	상	X	0.00	100.00	4
A.6.2	외부조직					
A.6.2.1	외부조직과 관련된 위험인식	중	X	0.00	100.00	4
A.6.2.2	고객과의 거래시 정보보안사항 전달	상	X	0.00	100.00	4
A.6.2.3	제3자 계약에서 보안사항 전달	상	X	0.00	100.00	4
A.7	자산관리					
A.7.1	자산에 대한 책임성					
A.7.1.1	자산 목록	상	X	0.00	100.00	4
A.7.1.2	자산의 소유권	상	X	0.00	100.00	4
A.7.1.3	자산 사용의 허용	상	X	0.00	100.00	4
A.7.2	정보 분류					
A.7.2.1	분류 기준	중	X	0.00	100.00	4
A.7.2.2	정보 라벨링 및 및 취급절차	상	X	0.00	100.00	4

4.3.2 위험평가 실시

1) 잠재적 위험 식별

기업의 업무 및 사용되는 시스템 등을 고려한 잠재적 위험 식별이 되어야 한다.

2) 잠재적 위험 평가

식별된 잠재적 위험에 대해 현재기업에서 적용한 보안통제 평가 실시.

3) 노출위험평가(Exposed Risk)

잠재위험에서 정의한 위험에 대응하기 위한 통제가 미흡하거나 부재로 인하여 발생할 수 있는 위험을 기입한다.

4) 위험지수(Risk Valuation) 평가

노출된 위험이 해당 자산에 미칠 수 있는 위험의 정도를 기밀성, 무결성, 가용성 측면에서 점수를 기입하며, 다음과 같은 기준을 참고하여 평가한다.

(1) 3점 : 노출위험이 실제로 발생했을 경우 기밀성, 무결성, 가용성 측면에서 전사적으로 중대한 손실을 미치는 경우

(2) 2점 : 노출위험이 실제로 발생했을 경우 기밀성, 무결성, 가용성 측면에서 전사적으로 부분적인 손실을 미치는 경우

(3) 1점 : 노출위험이 실제로 발생했을 경우 기밀성, 무결성, 가용성 측면에서 관계없거나, 손실을 발생시키지 않는 경우

5) 위험도 계산(Risk Calculation)

'중요성 평가/평가 등급'과 위험 지수(Risk Valuation) 값을 기밀성, 무결성, 가용성 각각에 대해 다음과 같이 정의한 수식에 따라 위험도를 계산하여 기입한다.

위험도 산출은 정성적 방법과 정량적 방법을 사용하고 있으나 본 연구에서는 정보자산 평가와 ISO 27001 보안통제 요구사항을 포함하여 전체적인 관점에서 위험평가를 실시하는 방법을 사례로 하였기 때문에 정성적 방법에 따라 다음과 같이 계산하였다.

・위험도(R) = 자산가치(A) + 위협(T) + 취약점(V)

<표 4.3> 위협 평가 기준

구분	값	의미
위협	VH	가능성이 매우 높음 (75% 이상의 확률)
	H	가능성 높음 (60% 이상의 확률)
	M	가능성 어느 정도 있음 (25% 정도의 확률)
	L	가능성 거의 없음(확률 거의 없음)
취약점	<표4.1> 참조	

해당 기업의 정보자산에 대한 위험도 평가 결과는 정보자산에 대한 가치(중요도)평가와 자산에 대한 위협, 취약점 평가를 실시하고, 이에 따라 위험도 평가를 실사하여 일정 수준 이상(Level 8이상)의 자산에 대해서는 관리 대상 위험으로 분류하고 수준이하의 자산에 대해서는 자산의 중요도가 낮거나 자산의 중요도가 높더라도 위협 및 취약점 수준이 낮아 업무에 미치는 영향이 낮음으로 분류하여 평가하였다.

<표 4.4> 위험도 평가 기준

위협		VL				L				H				VH			
취약점		VL	L	H	VH	VL	L	H	VH	VL	L	H	VH	VL	L	H	VH
자산가치	1	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	2	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10
	3	5	6	7	8	6	7	8	9	7	8	9	10	8	9	10	11

<표 4.5> 해당 중소기업의 위험도 평가 사례

자산 명	자산가치			등급	위협	고려 측면	위협 평가	취약성	취약성 평가	위험도		
	C	I	A							C	I	A
시스템 (그룹웨어)	1	2	2	6	외부 시스템과 연계	A	H	외부 시스템과 연계하여 어느 장소에서나 결재 가능토록 노출	L	6	7	7
시스템 (형상관리)	3	3	2	8	최신본 미 유지	I	H	정보시스템 획득, 개발에 형상관리시스템이 활용되나 전체적으로 활용되고 있지 않음	L	8	8	7
PC	2	1	1	4	해킹으로부터 침입, PC고장 장애	C	L	불법 소프트웨어 사용으로 악성코드에 의한 PC사용불가	H	7	6	6
정보 및 문서(기획문서)	2	1	1	4	기밀 유출	C	L	작업 중인 기획문서가 책상위에 방치	H	7	6	6
정보 및 문서 (개발문서)	2	2	2	6	최신본 관리	I	H	개발문서의 형상관리시스템 활용 부재로 동일 최신본 관리 되지 않음	L	7	7	7
정보 및 문서 (수주/계약)	2	2	2	6	외부인에 의한 정보 유출	C	H	가격, 마케팅정보 등 민감한 정보가 제3자에 의해 유출	L	7	7	7
정보 및 문서 (정보변경)	2	2	2	6	발주서의 데이터 실제 입력자 확인 불가능	I	L	구매발주문서의 잦은 변경으로 실제 입력데이터의 확인 불가능	H	7	7	7

4.3.3 위험 보안 대책 수립

위험평가 결과를 바탕으로 하여, '수용가능 위험 수준(DoA: Degree of Assurance)'을 정하며, 관리대상 위험을 식별하고, '수용가능 위험 수준(DoA)'을 근거로 관리대상 위험을 선정하고 '적용성 보고서(SoA: Statement of Applicability)'를 작성하여 의사결정권자에게 보고 및 관리한다.

적용성 보고서는 위험을 회피, 전이, 감소, 삭제 등의 대응방법을 정의하고 이에 대한 구체적인 관리 방법을 정의한다.

위험 대응방법에 따라 수용하기로 결정한 위험에 요소에 대해서는 그 사유를 남긴다.

'적용성 보고서(SoA)'에서 이행하기로 한 보안 통제 항목들에 대하여 구체적인 위험관리 방안을 수량화하고, '위험관리 계획서'를 작성한다.

<표 4.6> 보안 대응책 우선순위 사례

수행 과제명		평가기준			총점	우선순위	구분
과제	세부과제	효과성	긴급성	적용성			
정보보안관리체계 강화	정보보안 지침/프로세스 체계 보완	4	3	4	11	5	단기
정보보안조직체계 강화	보안관제 조직 등 강화	4	2	3	9	7	단기
물리적 보안 강화	보안구역 출입통제 강화(접근통제, 출입증)	5	4	5	14	2	중장기
	휴대용 장비 등 반출입 절차 수립	5	4	4	13	3	단기
PC보안 강화	PC보안 솔루션 강화	5	4	4	13	3	단기
	PC저장 데이터 보안강화(암호화)	2	2	2	6	10	단기
	고객 PC 보안강화 방안 대책 수립	5	4	4	13	3	단기
침해사고 대응체계 강화	침해사고 대응체계 수립 및 조직운영	5	5	5	15	1	단기
	로그분석 시스템 구축	4	3	4	11	5	단기
	통합 보안관리를 위한 시스템 구축	3	3	3	9	7	중장기

'적용성 보고서(SoA)'는 다음과 같은 사항을 포함하여 작성한다.

(1) 위험 통제 항목
(2) 통제 적용 여부
(3) 통제 적용 현황
(4) 통제 적용 계획
(5) 해당 위험 통제항목과 관련된 회사 내부 규정, 지침 및 절차

해당 중소기업의 산업보안경영시스템 구축과정에서 정보자산에 대한 가치평가, 위협 및 취약점 평가, 위험도 분석을 통해 일정 수준이상의 위험 대상에 대해서는 보안 대응책 우선순위를 효과성(과제 수행을 통해 보안 수준 향상에 미치는 정도), 긴급성(과제를 통해 보안 취약점 및 위험요소를 제거해야 하는 시급정도), 적용성(해당 기업환경에 과제의 안정적 적용 가능 정도)으로 구분하여 세부과제별로 우선순위에 따라 단기, 중장기 적으로 대응해야 하는 계획을 수립하게 되었다.

본 연구를 통해 산업보안 경영시스템 체계 구축을 위한 자산평가와 위협 및 취약점 평가, 이를 통한 위험도 계산을 하여 위험의 우선순위를 결정하고 이에 대한 대응책을 마련하기 위해 수용 가능한 위험 수준과 적용성 보고서를 작성하였으며, 산업보안 경영시스템 구축 전에 기업이 모니터링하고 통제하여야 할 주요 대응책을 정립하였다.

취약점 관점에서 본 주요 대응책은 1. 정보 및 문서의 보안등급이 분류되지 않아 문서 보안관리체계 확립이 시급한 과제로 정의되었으며, 2. 조직원이 사용하는 개인별 사무장비(노트북, PC 등)에 대한 보안인식이 부족하여 바이러스 백신 Update활동이 미흡하고, 3. 전사적 관점에서 보안감사 실시 및 시스템 보안 통제 적용이 미흡한 것으로 정의하였다. 끝으로 산업보안 강화 모델을 도출하는 의미에서 관리적, 기술적 및 물리적 보안의 취약점 분석을 통하여 도출된 각 보안 대책을 구현하기 위한 방안으로 몇 가지의 보완개선 모델을 도출하였다. '<표 4.7> 보안 강화 모델의 도출 예시' 참조

5. 결 론

본 연구에서는 산업 현장에서 발생하고 있는 각종 보안사고로 인하여 기업 경영활동에 막대한 손실이나 피해가 발생하는 것을 사전에 예방함으로써 그 피해를 최소화 하고 안정적인 기업 활동이 전개될 수 있도록 산업보안 경영시스템을 구축하여 조직 내에 적용함은 물론 개선 과제를 도출하여 지속적으로 산업보안 시스템이 발전하는 기회를 제공하고자 노력하였다.

정보자산의 가치를 평가하고 위협 및 취약점을 평가하기 위한 기준을 마련하는 것이 쉽지 않은 작업이었으며, ISO 27001 보안통제 요소와 물리적으로 구성되는 기업 자산과의 비교 평가를 통한 개선과제 도출까지는 경영자와 담당 조직원의 노력이 없이는 쉽게 접근하기 어려운 과제였다.

또한, 해당 기업의 정보자산 중 기업의 기밀보안 문서나 사업계획 등을 프로젝트 추진 과정에 공개해야 하는 어려움과 프로젝트 수행 인력에 대한 정보보안 각서를 서명하였음에도 불구하고 해당 기업의 조직원과 신뢰를 획득하는데 까지 많은 시간과 노력이 필요한 것은 개인의 신뢰보다 사회 저변에 깔려 있는 막연한 불신의 벽이 더 크게 느껴졌다는 데 아쉬움이 있었다.

따라서, 산업보안 경영시스템 구축과 내실 있는 실행을 위해서는 해당 기업의 조직원에 대한 보안 교육이

<표 4.7> 보안 강화 모델의 도출 사례

관리적 보안 강화 방향														기술적 보안 강화 방향												물리적 보안 강화 방향						
전사 정보보안정책 수립 및 사내 공표	보안정책 이행을 위한 세부 보안관리 규정/지침 마련	정보보안 정책의 지속적인 이행 점검 및 개선	전사 정보보안 심의기구 설치 및 운영	정보보안 실무자 협의회 구성 및 운영	외부인력 보안관리 강화	정보보안 전담부서 운영 및 보안관리 인력 확보	정보자산 관리강화 및 위험 평가	내부 직원의 보안관리 강화	연간 정보보안 교육 및 훈련 계획 수립 및 이행	정보보안 침해사고 대응 및 복구체계 수립	정보시스템 개발 시 보안성 검토 시행	안전한 웹 프로그래밍	개인정보 보안 관리 강화	패스워드 관리정책 강화(서버/NW)	시스템 사용자 권한분리/통제	통신 암호화 체계 강화	서버 접근통제 강화	서버 보안설정 강화	서버 로그 및 모니터링 활동 강화	주기적인 취약점 진단(서버/NW)	네트워크 보안설정 강화	네트워크 접근통제 강화	네트워크 분리 및 이중화	통신암호화 체계 강화	NW 로그관리 및 모니터링 강화	물리적보안 정책수립 및 사업장별 침입 운영 지	보안구역수준에 따른 출입통제 강화	사업장내 주요 자산 보안 강화	사업장 출입동선 통제 강화	IT인프라 연계된 물리보안 시스템 설치/운영	보안사고 대비 증거기록의 확보/관리	보안 강화 방향 / 보안 구현 모델
●	●	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	정보보안 정책 운영 강화
○	○		●	●		●		○		○																						정보보안 조직체계 수립
○	○					○	●													○												정보자산 위험평가체계 강화
○	○				●			●	●			○														○	○					정보보안 교육/훈련 강화
○	○					○				●									○						○							○ 보안 침해사고 대응 체계 수립
○	○	●					○				○									●						○	○	○	○			○ 정보보안 이행점검 및 진단 강화
○	○				○			○																		●	●	●	●	●	●	물리적 보안 관리 체계 강화
	○													●	○		○			●	●	●	●	●	●							네트워크 보안 강화
	○																	○	●	○					●							로그 백업 및 분석 강화
	○													●	●	●	●	●	●	●		○		○								서버 보안 강화
	○				○			○					○															●			○	사용자 보안 강화
	○											●								○												대외 웹서비스 보안강화

(●: 해당 '보안대책'과 '강화모델'이 직접관련)
(○: 해당 '보안대책'과 '강화모델'이 간접관련

선행되어야 함은 물론, 보안에 대한 사회적 인식이 함께 뒤따르고, 기술적 보안과 관리적 보안에 대한 기술적 대응 노력이 무엇보다 중요한 것임을 깨닫게 되었다. 범 국가적인 차원에서 산업기술의 유출방지 및 보호에 관한 법률(지식경제부 법률 2P9368호, 2009.1.30 일부개정)이 제정되어 전 산업군에 적용되고 있으나 이보다 선행하여 지켜져야 할 것은 산업보안에 대한 인식이 변해야 할 것이며, 산업기술의 발달과 함께 산업보안 관리 및 통제 수단도 함께 발전하는 기회가 사회 전반적으로 확산될 수 있기를 기대된다.

6. 참 고 문 헌

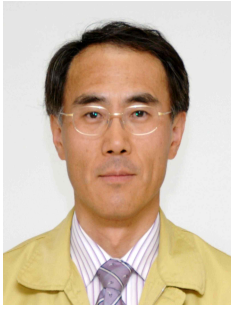
[1] 지식경제부, "산업기술의 유출방지 및 보호에 관한 법률" 2009.1.30
[2] 한국산업기술보호협회 권태종, "산업보안 특강", 2009. 9
[3] 기술표준원, "'중소기업을 위한 정보보안경영시스템(ISO 27001) 가이드라인", 2007.12
[4] 한국정보보호센터, "정보보호 개론", 2000.2 교우사
[5] 홍승필, 고재욱 "정보보안 기술과 구현", 파워북
[6] 정보보호 21C, "기업정보보호 실천 가이드", 2001.8
[7] 국가정보원, "첨단 산업기술 보호동향", 2009.5
[8] 고준철, "산업보안관리체계 구축을 위한 위험평가 및 위험처리에 관한 연구", 대한안전경영과학회, 2009.11
[9] 신동훈, "정보보호 사전진단 방법론을 활용한 u-City 보안 모델 연구", 2010.02
[10] 이영규, "정보보안 평가지표의 부합성 및 중요도에 관한 실증연구", 2008. 02
[11] ISO/IEC, "ISO 27001:2005 국제표준 규격", 2005

저 자 소 개

고 준 철

홍익대학교에서 석사를 취득하였고 현재 AB&S(주)컨설팅 사업부 이사로 재직 중으로 IT산업 분야의 컨설팅 서비스와 교육훈련 강사로 활동하고 있으며, 주요 관심분야는 IT Governance, ISP/BPR, 정보보안경영시스템 구축, 소프트웨어 프로세스 개선(SPI) 분야로 현재 명지대학교 박사과정에 재학 중에 있다.
주소: 경기도 안양시 만안구 안양6동 호정타워 212호

김 태 수



경희대학교에서 석사학위를 취득하였고, 한국과학기술연구원 강릉분원에서 행정팀장으로 재직중이며, 이공계 대학 및 연구기관 실험실 안전관리 증진을 위해 (사)대학환경안전협회 이사로 활동하고 있으며, 주요 관심분야는 안전교육 및 훈련, 예방활동, 안전장비 및 시설유지의 시스템적관리에 대한 실험실 안전환경 조성과 연구활동종사자 건강관리이며, 현재 명지대학교 박사과정에 재학중이다.

주소: 강원도 강릉시 연곡면 영진리 380번지 부영@ 301동 501호

주 용 마

서강대학교에서 석사를 취득하였고 현재 웅비특수강(주) 대표이사로 재직중이며, 제조업 분야에서 부품사업 및 완성품 사업에 전념하며 관심분야는 기업의 생산성 향상 및 원가분석 분야이며 현재는 명지대학교 박사과정에 재학중이다.

주소: 경기도 용인시 수지구 동천동 동문아파트 303동 2002호

김 우 현

노동부 한국고용정보원(구 중앙고용정보원) 직업지도과장을 역임하며 한국직업사전(초판) 편찬·집필, 적성·흥미검사, 직업지도·상담 프로그램 등을 기획·개발했으며, 현재 한국산업인력공단에서 외국인취업교육팀장, 기업지원팀장, 능력개발기획팀장 등을 거쳐 현재 성남지사 HRD사업팀장으로 근무하고 있으며 명지대학교 산업경영공학과 박사과정에 있다.

주소: 경기도 성남시 수정구 수진동 4554 한국산업인력공단 성남지사 HRD사업팀

강 경 식

인하대학교 산업공학과에서 학사·석사·박사와 연세대학교·경희대학교에서 경영학 석사·박사 취득. North Dakota State Univ.에서 Post-Doc과 Adjunct Professor 역임. 현재 명지대학교 산업경영공학과 교수로 재직 중. 주요 관심분야는 생산관리, 물류관리, 안전경영 등.

주소: 경기도 용인시 처인구 남동 산 38-1 명지대학교 산업경영공학과