ESP와 컴퓨터 보안 위험 관리에 대한 연구
A Study of ESP and Computer Security Risk Management

안태희, 김영렬
충북대학교 경영정보학과

요 약

네트워크의 발달과 인터넷의 생활화로 컴퓨터 보안이 시대적인 중요문제로 부각하고 있다. 요즘 해킹으로 발생하는 재정적 손실은 특별하게 큰 사건이 아닌 경우에 언론에 보도되지 않을 정도로 만성적인 현상으로 인식되고 있으며 컴퓨터 범죄는 어느정도 사회현상의 하나로 여겨질 정도다.

그러나 컴퓨터 범죄를 퇴치하고 컴퓨터보안의 완벽성을 유지하고자 하는 기술적인 노력은 지속적으로 전개되고 있으나 컴퓨터 범죄는 오히려 늘어가고 있는 추세다. 이에따라 컴퓨터 범죄등 컴퓨터보안관리가 기술적인 수준에 머물지 않는 성격을 갖추고 있다는 인식이 최근들어 확산하고 있다고 할 수 있다.

이 논문은 이런 인식에서부터 출발해 새로운 개념으로 등장한 전사적 보안관리(Enterprise Security Planning)와 컴퓨터 보안 위험 관리(Computer Security Risk Management)의 개념에 대한 이해를 중점적으로 제기했다.

또 컴퓨터 보안위험관리의 과정을 단계별로 검토해 컴퓨터 보안위험관리를 체계적으로 이해할수 있도록 제시했다.

마지막으로 본 논문은 전사적 보안관리와 컴퓨터 보안위험 관리차원에서 기업이 보안관리를 위해 갖춰야 할 새로운 흐름들, 예를 들어 보안관리자(Chief Security Officer) 제도와 보안보험 가입등 보안정책을 제시함으로써 컴퓨터범죄로부터 기업이 최대한의 안전성을 확보할 수 있는 경영전략의 틀을 제시했다.

Ⅰ.서론

정보보안은 얼마나 강화돼야 충분할까? 오늘날 이 질문에 대해 만족할 수준의 대답을 할만한 사람은 아마 없을 것이다. 세계가 점차 정보화 되고 각각의 컴퓨터가 하나의 네트워크로 묶이면서 정보의 사용량과 함께 정보보안을 침해하는 사건이 크게 증가하고 있다. 매일 컴퓨터 범죄에 대한 소식을 듣게 되며 이런 범죄들은 전자상거래의 활성화를 막는 중요한 요인중의 하나로 인식되고 있다.

'2002 CSI/FBI Computer Crime and Security Survey'에 따르면 응답자의 90%가 최근 12개월간 컴퓨터 보안 관련 침해를 탐지한바 있으며 80%는 컴퓨터 침해사건으로 재정적인 손실을 본적이 있다고 응답했다. 또 1997년의 조사에서는 정보절도로 생긴 평균손실액이

954,666달러, 총손실액은 20,048,000달러였으나 2002년에는 평균손실액이 6,571,000달러, 총손실액이 170,827,000달러로 급증했다.[1]

바이러스 침해에 의한 재정적 손실은 1997년 총손실액이 12,498,150달러, 평균 75,746 달러였으나 2002년에는 총손실액 49,979,000달러, 평균 283,000달러에 이르렀다. 1997년부터 2002년까지 이 조사에 응답한 500여개의 정부, 회사가 입은 코드레드 등 바이러스에 의한 피해액만 1억5000만달러에 이를 정도다.

이에따라 해커로부터 정보자산을 보호하기 위해 쓰여지는 막대한 예산으로 전자상거래업체들은 큰 지장을 겪고 있으며 전자상거래를 하는데 엄두를 내지 못하게 하는 요소로 작용하고 있다.

그동안 정보보호에 대한 인식은 주로 기술적인 문제로 인식되어 왔다. 이런 인식은 기술이 컴퓨터 보안 문제를 해결할수 있다는 생각으로 그동안 인증, 방화벽등 수많은 신기술을 양산해왔다.

그럼에도 불구하고 컴퓨터 보안 침해사례는 오히려 늘고 정보보호의 미래는 그다지 밝지만은 않은 실정이다.

이에 따라 정보보호에 대한 기술적인 접근 대신 전략적인 접근이 필요하게 됐으며 이런 인식의 바탕에서 전사적 보안관리(Enterprise Security Planning)라는 개념이 탄생했다. 전사적 보안관리는 기업이 최대한 보안을 확보할 수 있도록 기업자체의 각종 요소들을 보안의 관점에서 관리해야 한다는 필요성을 제기하고 있다. 또 전사적 보안관리 차원에서 컴퓨터 보안을 체계적으로 관리할수 있도록 고안된 컴퓨터 보안 위험 관리(Computer Security Risk Management)도 새로운 영역으로 관심을 모으고 있다.

Ⅱ.본론

1. ESP

IMF관리체제가 도입된 이후 경영환경의 변화가 다양해지고 그 변화속도가 기하급수적으로 빨라지면서 기업이 노출되는 위험의 종류 및 정도가 급격히 증가하는데 대한 인식이 확산하고 있다.

이에 따라 전략적 경영목표로서의 새로운 위험관리 체계의 도입은 이제 국내 기업들에게 있어 증가되는 위험에 대하여, 또한 국제화된 경영환경에 적응하기 위하여 필수적인 과제로 떠오르게 되었다. 이는 기존 경영방식에서의 일부 개선 정도의 소극적 방법으로는 해결되지 않으며 통합적이고 계속적인 경영위험관리의 새로운 패러다임의 도입이 필요하게 된 것이다.[2]

특히 요즘처럼 네트워크가 컴퓨터와 파트너들에게 광범위하게 퍼진 상태에서 기업의 컴퓨터 보안이 100% 보장받기는 불가능하다. 그러나 제한적인 기술과 예산, 인적자원, 다른 요소들에 의해 100%에 가깝게 보안을 유지할 수는 있다. 기업이 보안계획을 갖는다면 그들의

목적은 컴퓨터 자원과 데이터에 대한 완전한 보안을 제공하는 것일 것이다.

이런 차원에서 기업에서의 전사적 보안 자원관리의 필요성이 증대하고 있다. 전사적 보안관리(ESP:Enterprise Security Planning)는 기업에게 가장 높은 수준의 보안을 유지할 수 있는 방법중 하나로 탄생했다. 전사적 자원관리는 보안 설계와 실행에 있어서 실질적인 과정과 방법론이며 기업의 보안문제에 대한 근본적인 철학적 문제들을 풀어주게 될 것이다.

ESP는 단순한 선형적인 과정이 아니며 6가지 과정으로 구성돼 있다. 첫째는 기업의 보안을 준비하는 단계, 두번째는 자원과 도메인에 의한 보안조직, 셋째 기초보안 분석의 완료, 넷째 요구조건의 완성, 다섯째 자원을 확인하고 우선순위를 정렬하는 것, 여섯째 프로젝트의 선택과 실행이다.[3]

2. Computer Security Risk Management

2.1 위험

일상생활에서 위험은 매일 만날 수 있는 성질을 갖는다. 위험(Risk)과 불확실성(Uncertainity)은 서로 깊이 연관돼 있으며 불확실성에 따라 발생하는 손실을 위험이라고 할 수 있다. 위험은 세 가지로 나눌 수 있는데 순(Pure Risk) 위험과 투기적 위험(Speculative Risk)으로 나눌 수 있다.

순위험은 손실이 발생할 것인가에 따른 불확실성이 존재하는 위험으로 이익이 발생할 가능성이 없는 위험이다. 순위험의 근원은 3가지 인데 재산위험과 신뢰성 위험, 생명 과 건강위험, 수익손실위험으로 나뉜다.

반면, 투기적 위험은 불확실성으로 인해 어떤 사건의 결과 이익이나 손실을 발생시킬 수 있는 위험을 말한다.[4]

또한 위험은 잠재적인 취약성을 수행할 있는 주어진 위협근원의 가능성의 기능과, 조직에서 반대적인 효과의 결과이다.[5]

이런 위험을 확인하고 측정하며 리스크를 받아들일 수 있는 수준까지 감소시키는 일련의 과정이 위험관리(Risk Management)이다. 위험관리는 한 조직의 정보를 담고 있는 시스템을 보다 안전하게 하고, 잘 수행된 리스크 매니지먼트 의사결정을 통해 매니지먼트를 수행하게 하는데 목적을 갖고 있다.[6]

그러나 위험관리는 어느 한 분야에만 국한된 것은 아니고 우리의 삶에서 의사결정을 하는데 있어 항상 나타나는 문제다. 요즘 많은 사람들이 가정안에 있는 가치있는 물건과 생명을 보호하기 위해 가정에 보안시설을 갖추는 것과 같다.

위험관리의 목표는 기업이 노출되거있는 위험에 대한 파악과 측정, 그리고 그 위험이 경영진과 주주가 감당할수 있는 수준으로 감소시키고 억제될 수 있도록 계속적으로 관리해 기업의 영속성을 보장하는 것이다[7]

위험관리는 위험확인과 측정, 평가, 감소와 통제를 하는 전 과정에 적용되는 단어이며 위

험인지, 위험측정, 위험 평가, 실행, 모니터 및 감사등 5단계로 구성돼 있다.[8]

2.2 Computer Security Risk Management

기업차원에서 성공적으로 IT 보안 프로그램을 실시하는 것은 핵심적인 정보자산의 보호에 대한 인식 능력에 달려있다[9]

IT분야에서 컴퓨터 보안(Computer Security)은 정보시스템 자원(하드웨어, 소프트웨어, 정보 및 데이터, 통신포함)의 무결성, 가용성, 기밀성을 유지하기 위해 자동화된 정보시스템에 취해진 보호조치를 말한다. [10]

또 정보보안(Information Security)은 가치있는 정보를 보호하기 위한 것은 인류가 생긴 것 만큼 오래됐다. 최근에는 유용성(Aavailability), 완결성(Integrity), 확실성(Authenticity), 비밀성(confidentiality) 등 4가지 주요요소를 갖추고 있어야 한다고 개념화되고 있다. [11]

IT분야에서의 위험 관리과정은 위험 측정(Risk Assessment), 위험완화(Risk Mitigation), 위험평가(Risk Evaluation) 등 세 가지 과정으로 구성돼 있다. 위험 관리는 IT 매니저에게 그들 조직의 목적을 수행할 데이터나 IT시스템을 보호하기 위한 능력을 얻거나 방어측정을 할 수 있는 경제적 비용이나 기능을 조절하는 과정이다.[12]

2.2.1 위험 측정(Risk Assessment)

위험측정은 위험을 분석하고 해석하는 과정으로 평가의 범위와 방법론 결정, 데이터 수집 및 분석, 위험분석결과 해석등 3가지 기본적인 활동으로 구성된다. 위험 평가의 범위와 방법론은 위험 관리에 소비한 총 업무량과 평가결과의 형태와 유용성을 정확하게 정의한 상태에서 실시해야한다. 데이터 수집 및 분석에서는 정보와 소프트웨어, 직원들, 하드웨어, 컴퓨터 설비같은 물리적 자산을 포함한 자산평가, 발생할 수 있는 손해나 피해정도를 평가하는 결과평가, 해를 끼칠 수 있는 요소 또는 사건등의 위협요소 확인등이 있다.

이런 위험분석과 함께 위협에 대한 시스템의 취약성을 감소시키는 어떤 행위나 장치, 기타 다른 대책들을 분석하는 안전대책 분석과 통제들 내의 취약성과 결점을 분석하는 취약성 분석, 위협요소가 생겨나는 빈도나 가능성을 평가하는 가능성 평가등이 있다.

위험측정 단계에는 9가지 단계가 있다. 1단계는 시스템 특성화(System Characterizations), 2단계 위협 확인(Threat Identification), 3단계 취약성 확인(Vulnerability Identification), 4단계 통제분석(Control Analysis), 5단계 가능성 판정(Likelihood Determination), 6단계 충격분석(Impact Analysis), 7단계 위험판정(Risk Determination), 8단계 통제추천(Control Recmmendations), 9단계 결과 문서화(Result Documentation)이다.

① 1단계-시스템 특성화

첫단계에서 IT에서 위험을 확인하기 위해서는 시스템 환경을 잘알아야 한다.이를 위해서

위협요소	동기	위협행동
해커, 크래커	도전 이기 반역	해킹 사회적 엔지니어링 시스템 침입 불법적 시스템 접근
컴퓨터범죄	정보파괴 불법적 정보폭로 금전적 획득 불법적 데이터변조	컴퓨터범죄(예:사이버스토킹) 사기 정보뇌물 시스템 침투
테러리스트	블랙메일 파괴 사기 복수	폭탄/테러리즘 정보전쟁 시스템공격 시스템 침투
산업스파이	경쟁적 이익 경제적 탐지	정보절도 개인정보 침해 사회적 엔지니어링 시스템침투 불법적 시스템 접근
내부자	호기심 에고 지능 금전적 획득 복수 비의도적 실수	근로자에 대한 공격 블랙메일 사적정보의 관찰 컴퓨터 범죄 사기와 절도 정보뇌물 부정적으로 틀린 정보 입력 가로채기 사악한 코드(바이러스등) 개인정보 판매 시스템버그 시스템 침투 시스템 사보타지 불법적 시스템 접근

<표1> 인간 위협 : 위협요소, 동기, 위협행동들

하드웨어, 소프트웨어, 시스템 인터페이스, 시스템과 데이터의 민감성등에 대해 측정하고 분류해 놓아야 한다. 이와 관련된 정보를 수집하기위해서는 설문조사를 하거나 온라인 상에서의 인터뷰, 문서리뷰, 자동 스케닝 기술을 사용할수 있다.

② 2단계-위협확인

이 단계에서는 위협의 근원들을 확인하고 잠재적인 위협요소들을 리스트하는 것이다. 위협요소는 IT 시스템에 잠재적인 손실을 줄수 있는 잠재적인 환경이나 사건을 일컫는다. 일반적인 위협요소로는 자연현상과 인간, 환경등이 있을 수 있다. 이 단계에서 중요한 것은 모

보안영역	보안기준
관리 보안	책임성 지원의 연속성 사고반응 능력 보안 통제에 대한 정기적 리뷰 인적 완벽성 및 배경조사 위험 측정 보안과 기술적 교육훈련 임무의 분리성 시스템권리 및 재권리 시스템이나 애플리케이션 보안 계획
기능적 보안	먼지등 공기함유물 통제 전기설비의 질 통제 데이터미디어 접근 시설보호 습도통제 온도통제 워크스테이션, 랩탑, PC
기술적 보안	커뮤니케이션 침입탐지 시스템 감사

<표2>보안 기준

든 잠재적인 위협요소들을 고려하는 것이다. 이중 인간의 위협요소로는 해커와 크래커, 컴퓨터범죄, 테러리스트, 산업스파이, 내부자등이 있다.

③ 3단계-취약성 확인

3단계에서는 위협을 분석하는데 있어 시스템과 관련된 취약성분석을 반드시 포함해야 한다. 취약성은 보안침해를 받거나 보안정책을 위반할 수 있을 정도로 시스템 보안과정이나 설계, 내부 통제의 약함을 말한다. 취약성 분석에서는 관리적차원, 작동적 차원, 기술적 차원에서 확인을 해야 한다.

④ 4단계-통제분석

이 단계의 목적은 시스템 취약성에 대한 위협연습 가능성을 최소화하기 위해 조직에 의해 실행된 통제들에 대해 분석하는 것이다. 이를 위해서는 취약성 확인에서와 마찬가지로 관리적, 작동적, 기술적 차원에서의 체크리스트를 확인하는게 도움이 된다.

⑤ 5단계-가능성판정

가능성의 수준을 측정하기 위해서는 위협요소의 동기와 능력, 취약성의 정도, 통제수단의 존재여부와 효과성을 종합적으로 따져야 한다.

⑥ 6단계-충격 분석

시스템의 취약성에 대한 실험을 통해 나타나는 충격의 수준을 분석하는 것으로 손실의 수준결과에 따라 충격의 수준이 높거나 중간이거나, 낮은 것으로 분석할 수 있다.

⑦ 7단계-위험판정

위험을 판정하기 위해서는 위험수준 메트릭스를 확보해야한다. 위험의 수준은 위협 가능성과 위협충격을 종합적으로 점수화한 것이다. 이를 위해 3*3, 4*4, 5*5 수준의 메트릭스를 만들 수 있다. 위협 가능성과 충격에 대한 고, 중, 저에 대한 점수를 정하고 이를 메트릭스화해 위험정도의 수준을 정하는 것이다.

⑧ 8단계-통제수단 추천.

이 단계에서는 위험을 감소시킬수 있는 통제수단에 대한 추천을 하는 것이다. 적절한 통제수단의 추천을 위해서 추천옵션들의 효과성, 조직의 정책, 안정성과 신뢰성등의 요인들을 갖춰야 한다.

⑨ 9단계-결과문서화

위험 측정이 완료된 후에는 그 결과들을 공식보고서로 문서화해야 한다.

2.2.2 위험완화(Mitigation)

위험을 분석한 뒤에는 적절한 제약내에서 관리할 수 있는 수준으로 위험을 줄이는 보안통제의 선택과 구현과 관계있는 위험완화가 있다. 위험 분석을 통해서 적절한 통제를 통해 위험을 완화할 필요가 있다. 적절한 통제를 위해서 관리자는 조직의 정책이나 법률, 규정, 안전성, 시스템 성능요구사항, 적시성과 정확성등의 요구사항, 보안대책의 생명주기 비용, 기술적 요구사항, 문화적 제약등의 여러 가지 요소들을 고려할 필요가 있다.

위험완화는 시스템 임무의 위험을 감소시키기 위해 경영층 관리에서 사용되는 시스템적인 도구다. 위험완화는 위험 가정, 위험 회피, 위험 제한, 위험 계획, 조사와 확인, 위험 전환등의 옵션들을 통해 이뤄질수 있다.

위험완화 전략 행동의 단계는 우선순위 행동에 대해(1단계) 추천된 통제옵션들을 평가하고(2단계), 비용-이익 분석을 통해(3단계) 통제수단(4단계)을 결정한다. 이어 5단계에서 책임을 지워주며 6단계에서 안전실행 계획을 개발하고 7단계에서 선택된 통제수단을 실행한다.

통제수단으로는 기술적 수단과 관리적 수단, 기능적 수단이 있다. 기술적 수단으로는 지원적 수단과 방어적 수단, 탐지와 회복수단이 있다. 지원적 수단으로는 인증(Identification), 보안관리, 시스템 방어가 있다. 방어적 기술수단으로는 인증, 접근 통제강제(Access Control Enforcement), 부인방지(Nonrepudiation), 보호된 의사소통 통신사적보호가 있다. 탐지 및 복구기술통제로는 감사, 침입탐지, 보안상태저장, 바이러스탐지 및 제거가 있다.

관리적 보안 통제수단 중 방어통제로는 보안책임, 시스템보안 유지, 개인보안통제 실행, 보안 인지교육이 있다. 탐지관리 보안통제로는 인적 보안 콘트롤 실행, 보안 통제의 정기적인 리뷰, 시스템 감사의 정기적 실행이 있다. 복구관리 보안통제로는 재해나 비상상태에서 시스템을 유지할 수 있도록 영속성을 부여하고 사고에 대한 반응 능력을 설비하는 것이다.

기능적 보안 콘트롤 중 방어수단으로는 외부 데이터배포 제한, 소프트웨어 바이러스 통제, 오프 사이트 저장과 보안, 랩탑 및 PC 보호등이 있다. 탐지기능 통제로는 폐쇄회로 TV등 물리적 보안시설과 화재 감지 장치등 환경보안 설비등이다.

위험완화에도 불구하고 위험이 잔재하는 수가 있다. 실제적으로 IT 시스템이 위험으로부터 자유로울 수는 없다. 그리고 통제수단들이 모든위험을 없애거나 위험수준을 제로상태로 만들수도 없다. 이에 따라 잔재위험을 최소화하거나 무력화하기 위해서 정기적인 보안 위험 관리가 필요하다.

2.2.3 평가와 측정

거의 모든 조직에서 네트워크가 확장되고 소프트웨어가 교체되고 있으며 이런 변화는 곧 표면적이거나 잠재적인 위험들이 되풀이될 수 있다는 것을 시사한다. 그렇기 때문에 보안 측정은 최소한 3년마다 실행될 필요가 있다. 그리고 성공적인 보안관리 프로그램은 경영자의 동의와 전폭적인 지원, 위험측정팀의 능력, 사용자의 협조, 위험에 대한 지속적인 평가와 측정이다.

Ⅲ.결론-효과적인 ESP를 구현하기 위한 제언들

컴퓨터 보안 위험 관리를 통해 효과적으로 전사적 보안관리를 하기 위해서는 기업이 자체적으로 보안조직의 위상을 격상시키고, 체계적인 조직의 틀을 갖춰야 한다.

보안을 강화하려는 회사는 반드시 보안 정책을 만들어야 한다. ESP를 하기 위해서는 이상적으로 필요한 것이 보안의 비즈니스적 필요성을 확인하고 보안정책의 범위를 정해야 한다. 또 보안관련 직무들을 분석해 정리해놓으며 재해복구등의 범위를 정해야 한다. 또 법적, 규정적 필요조건을 특화해야 한다.

특히 새로운 보안개념의 확산에 따라 보안관련 조직의 회사내 위치도 중요하다. 조직에서 보다 기술적이고 조직 통합적이며 CIO에게 직접 보고할 수 있는 체계를 갖춰야 한다.

또 보안관리자(CSO;Chief Security Officer)를 두어 보안조직의 위상을 높여야 할 것이다.

보안관리자에 대한 인식의 전환도 필요하다. 기술적인 것 뿐만 아니라 경영전략적 차원에서 관심을 가져야 하며 E-비즈니스 보험에 가입할 필요가 있다. 최근 보안 감시 서비스 업체인 Counterpane Internet Security Inc.는 자사의 고객들이 해킹으로 인해 손실을 입을 경우 이를 보상해 주기 위해 보험회사인 로이드사와 손잡기로 했다고 발표하는 등 컴퓨터 보안관리 분야에서의 보험이 영역을 넓히고 있다.

<참고문헌>

[1] Richard Power, "2002 CSI/FBI Computer Crime and Security Survey", *Computer Security Issues&Trends*, vol 8, Number 1, 2002

[2] -위험관리-전략경영의 새로운 패러다임,서울경제 1999년 3월29일

[3] Formulating an Enterprise Security Plan and an Introduction to Role-Based Authorization, Intel e-business Center White Paper.

[4] Trieschmann & Gustavson, Risk Management & Insurance. 9th edition, Southwestern. 1995

[5] Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30

[6] 전게논문, NIST Special Publication 800-30

[7] -위험관리-전략경영의 새로운 패러다임(서울경제 1999년 3월29일)

[8] S J Cox and N R S Tait, Reliability,Safety&Risk Management, Butterworth-Heinemann, 1991.

[9] ITL Bulletin February 2002

[10] AN Introduction to Computer Security: The NIST Handbook,(Special Publition 800-12), NIST,1999

[11] Donn B. Parker, Fighting Computer Crime: A New Framework For Protecting Information, John Wiley & Sons, Inc. 1998

[12] NIST Special Publication 800-30