조직 정보 시스템 보안을 위한 총괄 전략 프레임워크

박 상 서*

요 약

정보 시스템 보안 체계를 보다 체계적으로 구축하고 효율적으로 운영하기 위해서는 보안에도 전략이 도입되어야 한다. 또한, 전략이 구현되어 성공적으로 작동하기 위해서는 조직 차원의 참여가 필수적이다. 하지만, 조직의 정보 시스템 보안 전략에 관한 연구는 아직까지 전략적 사고에 의한 보안 체계의 배치와 운영에 초점이 맞추어져 있어, 조직 전체를 움직이고 이끌기 위한 총체적 프레임에 관한 연구는 부족한 실정이다. 따라서 본 논문에서는 조직 차원의 보안 전략 수립에 활용할 수 있는 프레임워크를 연구한다. 이를 위하여 조직 차원의 전략 수립이라는 측면에서 총괄 전략의 개념을 도입하였으며, 총괄 전략이 갖는 4차원적 특성을 기반으로 정보 시스템 보안 총괄 전략을 구성하기 위한 프레임워크를 제시한다.

Grand Strategy Framework for Information Systems Security in Organizations

Sangseo Park*

ABSTRACT

Strategies have to be employed in information systems security in order to build and operate systems for information systems security in effective and structured manner. It is also essential for the entire organization to participate for successful implementation of the strategies and making them work. Current researches on information systems security strategy in organizations, however, have mainly been focused on deployment and operation of countermeasures based on strategic thinking and decision. In consequence, it is lack of research on overall frame for containing consideration factors required for moving and leading the whole enterprise for the holistic security purpose. Therefore, this paper proposes a framework for use in establishment of organization-wide information systems security strategies based on the concept of grand strategy from the traditional strategy research and on the four dimensional features of it.

Key words : Grand Strategy, Information Systems Security Strategy

접수일 : 2009년 4월 3일; 채택일 : 2009년 6월 12일

* ETRI 부설연구소

1. 서 론

정보 시스템이 사회 전반과 기업 활동, 그리고 나아가 국가의 운영에까지 그 활용도가 급속히 증가하면서 정보 시스템 보호에 관한 관심이 높아지고 있다. 특히, 조직에서는 정보 시스템 보안의 중요성에 관한 인식이 널리 퍼지면서 다양한 노력이 지속되고 있다. 그럼에도 불구하고 사고는 계속 발생하고 있으며 피해 역시 줄어들지 않고 있다. 특히, 정보 시스템 보안에 있어서 하드웨어보다는 소프트웨어가 상당부분을 차지하는 현실을 볼 때, 소프트웨어가 가질 수밖에 없는 취약성 때문에 대부분의 정보 시스템은 안전하지 않을 수밖에 없으며[1], 조직의 생산성 향상 등을 꾀하기 위하여 새로운 정보 기술을 조직에 도입하는 것조차 새로운 위협을 예고하고 있는 실정이다[2].

Computer Security Institute에서 522개의 미국 기업, 정부 기관, 금융 기관, 의료 기관, 대학 등의 보안 전문가를 대상으로 조사한 바에 따르면[3], 응답자의 97%가 바이러스 백신 소프트웨어를, 94%가 방화벽을, 71%가 자료 전송시 암호화를, 그리고 53%가 하드 디스크에 자료 저장시 암호화를 사용하고 있다. 하지만, 응답자의 49%가 바이러스 공격을 받았으며, 27%는 "Targeted Attack"을 경험하였고, 전체 IT 예산 대비 정보보호 예산이 5% 미만인 조직은 전체 응답자의 53%에 달했다. 또한, 영국 소기업연합회(Federation of Small Businesses)의 조사에 따르면[4], 응답자의 84%가 방화벽을 사용하고 있고 52%가 보안패치를 적용하고 있으나, 응답자의 57%가 최근 12개월 동안 피해를 당하였으며, 특히 심각한 것은 피해 기업의 1/3이 이러한 피해를 신고하지 않았다는 것이다. Symantec사에서도 최근 523개의 미국 기업을 대상으로 조사한 결과[5], 응답자의 46%가 지난 2년간 사이버위협이 증가하였다고 답하였으며, 88%의 기업이 지난 2년간 공격을 받았다고 대답하였다. 특히, 67%의 기업이 사이버공격을 기업이 직면하고 있는 위험의 1, 2순위로 지목하였고, 49%는 보안이 더 어려워지고 있다고 응답하였다는 것이다. 그나마 응답자의 95%가 매년 정보보호 예산을 전년도와 유사하게 책정하거나 증액하겠다고 Enrst and Young의 설문에 응답한 것은[6] 다행이라 할 수 있다.

이러한 현상을 해결하고자 많은 대책들이 제시되어 왔으나 아직까지도 기술 연구에 중점적으로 초점이 맞추어져 있다. 지난 20여 년간, 주요 국제 정보 보호 학회에서 발표된 기술에 관한 논문의 수는 계속 증가하고 있으며[7], 기술개발에 대한 투자 역시 계속 강조되고 있다[8, 9]. 하지만 분명한 것은 기술적 접근만으로는 보안을 위한 노력이 실패할 수밖에 없다는 것이다. 정보 시스템 보안이 기술 중심적 사고를 뛰어 넘어 관리와 제도의 물결에 이은[10] 제 4의 물결인 정보 시스템 보안 거버넌스로 향하고 있는 상황에서[11] 기술 이외의 주제 특히 정보 시스템 보안 기술과 대책을 효율적으로 활용하기 위한 전략에 관한 관심과 주목이 필요하다[12]. 그리고 이러한 움직임은 학자들의 주장이나 학술적 지적을 넘어 조직의 정보 시스템 보안 전략으로 또는 IT 전략이나 비즈니스 전략에 포함되어 문서화되어 가고 있다[6].

정보 시스템 보안 전략이 조직내에 구현되기 위해서는 위협의 정도와 빈도, 보호해야 할 자산과 정보의 가치와 분량, IT 인프라 등 각 조직이 처한 상황과 환경에 따라 적절한 전략이 채택되어야 한다. 그리고 채택된 전략을 문서화하고 구현하여 그 효과를 창출하기 위해서는 조직 차원의 지원과 협조가 필수적이다. 즉, 조직 구성원의 공감대가 필요하며, 담당 조직의 편제와 함께 전문 인력의 확보와 양성도 추진되어야 하고, 적정 규모의 예산도 지원되어야 하는 등 전략을 조직내에 구현하기 위해서는 여러 고려사항들이 존재한다. 하지만, 전략에 관한 기존 연구는 전략적 관점에서 보안 대책의 배치를 통한 보안 체계의 구축을 중심으로, 전략의 도입 효과와 도입 방법, 전략 구현의 성공

요인 등에 관한 연구가 주를 이루고 있을 뿐, 기술의 적용과 운용보다 한 차원 상위에서 조직 전체의 방향을 설정하는데 사용할 수 있는 프레임워크에 관한 이론적·학술적 연구는 찾아보기 어렵다.

따라서 본 연구에서는 전통적인 전략 연구에서 제시하는 총괄 전략(Grand Strategy)[13-16]의 개념과 총괄 전략의 4차원 모델[17, 18]을 활용하여 조직 차원의 정보 시스템 보안 전략 수립시 고려하여야 할 여러 요소들을 종합적으로 표현할 수 있는 프레임워크를 제시하고자 한다. 그리고 이 프레임워크의 적절성을 검토하기 위하여 미국과 우리나라에서 2003년 발표된 국가 차원의 전략과 종합계획이 이 요소들을 포함하고 있는지 조사한다.

본 논문은 세 부분으로 구성되어 있다. 먼저, 정보 시스템 보안 전략의 개념을 설명하고 정보 시스템 보안 전략에 관한 기존 연구를 정리한다. 두 번째 부분에서는 조직 전체 차원에서 정보 시스템 보안 전략을 다루기 위한 개념으로서의 총괄 전략을 설명한다. 마지막으로, 세 번째 부분에서는 총괄 전략의 프레임워크를 제시하고 평가한다.

2. 정보 시스템 보안 전략에 관한 기존 연구

2.1 정보 시스템 보안 전략

정보 시스템 보안 총괄 전략을 논의하기에 앞서, 먼저 정보 시스템 보안 전략의 개념을 정립할 필요가 있다. 이를 위해서는 정의와 특성을 파악하는 것이 효과적일 것이다. 하지만 아직까지 정보 시스템 보안 분야의 전략은 개념 정립 단계에 머무르고 있다. 따라서 전통적인 전략과 연계하여 정보 시스템 보안 전략을 살펴보고자 한다.

Evered[13]에 따르면 전략은 주로 경영 관리, 군사 그리고 미래학(future research) 분야에서 주로 다루어져 왔지만 그 대상 영역과 연구자의 관점에 따라 각기 조금씩 다른 정의를 내리거나 핵심요소 또는 키워드를 제시하여 왔다. Evered[13]의 분석을 중심으로 경영 관리 분야를 먼저 살펴보면, Mintzberg[19]는 "의사결정 흐름의 패턴"(p. 935)으로 정의하였고, Chandler[20]는 '장기적인 측면에서 목적과 목표의 결정, 행동 양식의 채택, 그리고 자원의 할당'으로 정의하였다. Andrews[21]는 '목적을 정의하고, 정책과 계획을 수립하며, 기업활동의 범위와 조직의 정체성 등을 정의하는 의사결정의 패턴'으로 정의하였고, Salveson[22]은 '목표와 목적, 행동 양식, 그리고 자원·권한·업무 할당을 설정하는 것'으로 정의하였다. 반면, 군사 분야에서 Clausewitz[23]는 "전쟁의 목적을 달성하기 위하여 전투를 수행하는 것"[13](p. 63)으로 정의하였으며, Liddell-Hart[24]는 "군사적 수단을 배치하고 적용하는 것"(p. 335)으로 정의하였고, Reiter and Meek [15]은 '분쟁 해결의 수단'으로 정의하였다. 앞에서 언급된 두 분야에 비해 많은 주목을 받은 분야는 아니지만, Evered[13]는 미래학 연구에 있어서의 전략을 '행동 결정을 위한 도구'(p. 66)로 정의하였다.

정보 시스템 보안의 측면에서 보면, Saydjari[25]는 조직의 관점이라기보다는 군사적 또는 국가적 관점에서 "방어적 정책과 형상 및 공격 상황에 따라 작전 수행에 필요한 변화의 측면에서 좋은 결정을 내리는데 필요한 지식"(p. 54)으로 정의하였다. 반면, Park and Ruighaver[26]는 "기밀성, 무결성, 가용성을 보장함으로써 효과적이면서도 최소한의 노력과 비용으로 내·외부 공격으로부터 조직의 정보 인프라를 보호하기 위하여 어떠한 방어적 보안 기술과 수단을 어떻게 배치하여 적용할 것인가를 결정하는 술(術, Art)"(p. 27)로 정의하였다.

지금까지 살펴본 여러 정의와 연구 결과를 종합적으로 살펴보면, 경영 관리 분야는 대체적으로 기업이 나아가야 할 '방향과 목표의 설정과 계획의 수립'에 초점을 맞추고 있는 반면, 군사 분야에서는 주어진 목적이나 목표를 달성하기 위하여 '수단을 배치·운용하는 것'에 보다 초점이 모아지고 있는

것을 알 수 있다[12, 26]. 이 분석 결과를 조직의 정보 시스템 보안에 적용하면, 조직의 정보 시스템 보안 전략은 기업 활동이라는 측면에서는 그 영역이 비즈니스의 영역에 속하지만, 그 특성은 목표의 설정보다는 목표 달성을 위한 수단의 활용이라는 군사적인 분야에 가깝다는 것을 알 수 있다. 즉, (상위의 전략 개념인 기업 전략과 정보화 전략 등을 통해) 이미 정보 시스템 보안의 목표와 목적이 정해져 있기 때문에 경영 관리에서처럼 보안의 목표나 목적을 형성해가기보다는 주어진 자원과 수단을 어떻게 활용하여 보안을 유지할 것인가가 더 중요하다는 의미이다. 이러한 검토 결과는 Park and Ruighaver[26]의 정의에도 적절히 반영되어 있다.

앞에서 언급한 것처럼 정보 시스템 보안 전략이 내 · 외부의 공격으로부터 조직의 정보와 정보 인프라를 보호하기 위한 것이라고 보았을 때, 정보 시스템 보안 전략이 갖는 또 다른 중요한 특성은 방어적이어야 한다는 것이다[12]. 전략은 공세적이거나 방어적일 수 있는데, Posen[14], Reiter and Meek[15], 그리고 Reiter[27]은 공세적 전략을 '적을 파괴하는 것', 그리고 방어적 전략을 '적이 자신의 목적을 달성하지 못하게 하는 것'이라고 설명하고 있다. Agrell[28]은 공세적 전략을 '적진에서 전쟁을 수행하는 것'으로, 방어적 전략을 '아진이나 국경에서 전쟁을 수행하는 것' 또는 '적이 공격하는데 어려움을 겪게 하는 것'으로 설명하고 있다. 이와 같은 주장을 종합적으로 검토할 때, 정보 시스템 보안 전략은 조직의 정보 시스템에 대한 공격자가 그 목적을 달성하지 못하도록 하는 것이고, 전략이 실행되는 공간은 조직이 관할하는 정보 시스템 즉, 조직 내부의 시스템과 내·외부 접경지역이지만 조직에서 관리하는 시스템이다. 그리고 본 논문에서 의미하는 방어적 개념은 방어적 방어(Defensive Defense)이다. 즉, 방어를 목적으로 하는 선제공격(Strike-first)이나 보복공격(Strike-back)과 같은 적극적 방어(Offensive Defense 또는 Active Defense)는 군사적 충돌이나 국가간 분쟁 등의 사안에서는 충분히 검토될 수 있는 대안이겠지만, 일반적인 조직에서는 선택할 수 없는 방안이기 때문이다.

2.2 정보 시스템 보안 전략에 관한 연구 결과

정보 시스템 보안 분야에도 전략의 개념이 도입되어야 한다는 지적은 계속적으로 주장되어 왔다. Sherwood[29]는 기업에서의 정보 시스템 보안은 전략적 고려 없이 전술적인 측면에서 포인트 솔루션(Point Solution)들이 사용되어 왔음을 지적하며 각종 도구들의 숫자가 계속 증가할 경우 여러 도구들간의 상호운영, 관리의 어려움 등의 문제에 직면하게 될 것이므로 전략을 도입하여야 한다고 주장하였다. Edwards and Willimas[30]는 보안에서 전략이 간과되어 왔음을 지적하며 전략이 도입되어야 함을 언급하였으며, Saydjari[25] 역시 보안 대책들을 효율적으로 관리하기 위해서는 전략이 필요하다고 주장하였다.

조직의 정보 시스템 보안에 적용 가능한 전략에 관한 연구로, Grance et al.[31], Mell et al.[32], Walt[33], 그리고 Bowen et al.[34] 등 여러 전문가들은 각 조직이 보안 위협에 잘 대처하기 위해서는 봉쇄(Containment)와 같은 적절한 전략을 개발·적용하여야 한다고 지적하였다. Alberts[35]는 정보전(Information Warfare) 입장에서 전략 개발을 주장하였는데, 보안 수단의 개발보다는 전략의 개발이 우선시되어야 한다고 지적하였고, 동시에 종심 방어(Defense-in-Depth) 전략의 활용과 함께 억지(Deterrence) 전략의 개발이 필요하다고 주장하였다. Tirenin and Faatz[36]는 사이버전(Cyberwar)의 입장에서 기존 전쟁에 활용되는 전략을 사이버공간에 차용하여 억지, 종심방어, 기만(deception), 동적 격리(Dynamic Compartmentalization), 그리고 공격자 고립(Isolation of Attackers) 전략을 소개하였다. Tinnel et al.[37] 역시 사이버전 관점에서 적용 가능한 전략을 연구하였는데, Cyberwar

Playbook을 개발하여 공격자와 방어자가 각각 자신의 입장에서 공격과 방어에 사용할 수 있는 전략들을 검토하고 분석하였다. 특히, 공격자와 방어자가 서로 상대방에 대한 정보를 수집하는 모니터링(Monitoring) 전략과, 상대방을 속이기 위한 기만 전략을 중점적으로 소개하였다. Hamill et al.[38]은 정보보증(Information Assurance)의 측면에서 전략을 평가하기 위한 프레임워크를 제시하기 위한 연구를 수행하였는데, 비록 군사적 특성 때문에 스케일이 크고 복잡하여 일반 기업에 적용하기는 어렵겠지만, 구체적 기법으로 이형성(Heterogeneity), 정적 자원 할당(Static Resource Allocation), 동적 자원 할당(Dynamic Resource Allocation), 중복(Redundancy), 신속 복구(Rapid Recovery Reconstitution), 기만 등 열두 가지 전략을 제시하기도 하였다.

이와 같이 다양하게 제시되어 온 전략들을 분류하기 위한 방법에 관한 연구도 진행되었는데, 박상서[12]에 따르면, Parker[39], Kankanhalli et al.[40], Straub[41], Forcht[42]는 전략을 억지와 예방(Prevention)으로 구분하였고, Straub and Welke[43]는 억지, 예방, 탐지(Detection) 및 보수(Remedy)로, Lampson[44]은 전략의 기능에 따라 고립(Isolation), 축출(Exclude), 제한(Restrict), 복구(Recover), 그리고 처벌(Punish)로 구분하였다. 또한, Yang et al. [45]은 사전(Proactive)과 사후(Reactive) 전략으로 구분하였으며, Armstrong et al.[46]과 Mirkovic and Reiher[47]는 예방과 사후 전략으로 구분하였고, Smith[48]는 억지, 탐지, 지연(Delay), 그리고 대응(Response)으로, Ölnes[49]는 예방, 한정(Limitation) 및 정정(Correction)으로 구분하였다. 또한, Hamill et al.[38]은 예방, 탐지, 그리고 대응(reaction)으로 구분하기도 하였다. 나아가, 박상서[12]와 Park and Ruighaver[26]는 전략의 분류에 관한 초기 연구에서 정보 시스템 보안 전략을 적용 시기, 적용 지점, 그리고 의사결정 프로세스에 따라 구분하였는데, 적용 시기에 따라서는 사전 및 사후로 세분화하고, 적용 지점에 따라서는 경계선 방어와 종심 방어로 구분하였으며, 의사결정 프로세스에 따라서는 인지(Cognitive), 결정(Determinative), 그리고 지시(Directive)로 세분화하여 기존 분류에 비해 보다 체계적인 분류체계를 제시하였다.

그렇다면 조직의 정보 시스템 보안에 전략을 도입하면 과연 효과가 있을 것인가? 전략의 적용 효과에 관한 연구로, Straub[41]는 조직에 적용 가능한 정보 시스템 보안 전략으로 억지와 예방 소프트웨어의 적용을 제시하고, 1,211개의 조직으로부터 입수한 자료를 바탕으로 이들 전략을 적용할 경우 보안이 향상된다는 것을 실증적으로 보였다. 그 후, Straub and Welke[43]는 1990년도의 연구결과를 확장하여 적용 전략을 억지와 예방에서 억지, 예방, 탐지 및 보수로 확대하고, Fortune 500대 기업 2개에서 각각 인터뷰와 Action Research를 수행하여 전략의 활용이 보안을 향상시킨다는 것을 다시 한 번 입증하였다. Kankanhalli et al.[40]은 조직에서 사용할 수 있는 전략으로 제재의 확실성(Certainty of Sanction) 측면에서의 억지 노력(Deterrence Effort), 제재의 심각성(Severity of Sanction) 측면에서의 억지 정도(Deterrence Severity), 그리고 예방 노력(Preventive Effort)을 제시하고, 이것들이 조직에 구현될 때 고려하여야 할 요소로 조직의 크기, 최고 경영자, 그리고 기업 유형을 제안한 뒤, 실험을 통하여 억지 노력과 예방 노력은 정보 시스템 보안에 효과가 있음을 발견하였다. 그 밖에도 Gorman et al.[50]은 일반적인 보안 전략보다는 보호해야 할 대상을 특정하는 Targeted Defense가 효과적임을 지적하기도 하였다.

정보 시스템 보안에 전략을 도입하는 것이 의미가 있다면 어떻게 도입하여야 할 것인가? 이 질문에 답하기 위한 전략의 도입 방안에 관한 연구로, Sherwood[29]는 기업의 비즈니스 요구사항을 분석하는 것부터 시작하여 전략을 수립하고 이에 따라 서비스를 설정한 뒤 도구를 도입하는 SALSA

모델을 제시하였고, Liu[51]는 세 가지 측면에서의 다차원 대책(Multi-group Involvement, Multi-dimensional Security Mechanism, 그리고 Multi-layer Defense)의 필요성을 지적한 뒤, 보안 메커니즘은 예방, 탐지, 대응의 3단계 전략으로 구성하고, 보안 전문가뿐 아니라 일반 사용자와 매니저도 참여하며, 경계선(Perimeter), 서버, 그리고 데스크탑으로 다중 보안 계층을 구축하는 방안을 제시하였다.

그리고 전략을 조직에 구현할 때 고려하여야 할 성공요인에 관한 연구도 찾아볼 수 있다. Torres et al.[52]은 스위스 치즈 모델[53]을 이용하여 정보보안 인식(Infosec Awareness), 직원의 경쟁력(Staff Competence), 정보 시스템 보안 아키텍처, 정보 시스템 보안 전략, 정보보안 효율성에 대한 동적 평가, 보안 예산 등 열 두 가지 항목을 식별하였다. Wood[54]는 정보 시스템 보안 관리를 위한 조직 구조와 관리자의 인식 수준 측면에서 시스템 보안에 대한 책임감(Responsibility for Systems Security), 최우선 책임 부서(Primary Groups Responsible), 보고관계(Reporting Relationship), 관리 계층구조상의 직위(Level in Management Hierarchy), 책임 할당(Assigning Responsibility), 적절한 피드백 전달(Providing Proper Feedback) 등 열 네 개의 항목을 식별하였다. Kankanhalli et al.[40]은 조직의 크기, 최고 관리자의 지원, 기업의 유형, 예산규모 등 일곱 가지의 항목을 식별하였다. 이들 세 연구의 공통점은 정보 시스템 보안의 조직내 구현을 위한 성공요인을 조직의 측면에서 접근하였다는 것이다. 반면, 박상서와 박춘식[55]은 정보 시스템 보안 전략 자체가 가져야 할 요건에 관한 초기 연구를 통해 통합(Alignment), 균형(Balance), 효율성(Effectiveness), 비용(Cost) 등 열 두 가지를 식별하였다. 한편, Grance et al.[31]은 적절한 전략을 선택하기 위한 기준으로, 정보 시스템에 대한 잠정적 피해, 증거 확보 필요성, 전략 구현에 필요한 시간과 요구자원 등 여섯 가지를 제시하였다.

3. 정보 시스템 보안 총괄 전략의 개념

3.1 정보 시스템 보안 전략에 관한 기존 연구의 한계점

Agrell[28]은 군사적인 측면에서, 전략적 수준이라는 것은 군사적인 자원 전체와 관계된다고 지적하였다. 이를 정보 시스템 보안에 적용하면 조직으로부터 부여된 정보 시스템 보안의 임무를 수행하기 위하여 보안 담당 부서의 모든 역량과 자원을 활용하는 것이 된다. 하지만, 이것만으로는 부족하다. 전쟁의 수행을 위해서는 국가적 역량이 총동원되어야 하듯이, 정보 시스템 보안을 위해서는 조직 전체의 역량이 집중되어야 한다. 하지만, 앞에서도 정리된 바와 같이 정보 시스템 보안 전략에 관한 기존 연구는 보안 수단의 배치와 운영 측면에서 전략들을 제시 · 분류하고, 전략 적용의 효과를 검증하며, 전략을 조직내에 성공적으로 구현하는데 필요한 요소를 파악하는 것 등이 주를 이루고 있을 뿐, 전사적 차원에서 전략을 개발하여야 한다는 측면에서 기본적인 밑그림을 구상하기 위한 틀과 주요 구성 요소에 관하여 논의한 결과는 아직까지 찾아보기 어렵다.

전략적 마인드를 가지고 보안 기술과 도구를 적절히 배치하고 운영하는 것은 매우 중요하다. 하지만 보안 체계를 운영하기 위한 전문 인력과 조직의 구성이라던가, 구성원의 인식 향상과 합의 도출, 제도의 마련 등을 아우르는 종합적 측면에서의 학술적 접근은 아직까지 찾아보기 어렵다. 비록 Sherwood[29]와 Liu[51]가 조직 내에 보안 전략을 구현하기 위한 프로세스를 제시하고는 있지만 전체적 맥락에서 채택된 보안 전략이 적절히 효력을 발휘하게끔 여러 관련 요소들을 담아내기 위한 프레임워크를 제시하고 있지는 않은 실정이다. 이는

조직의 정보 시스템 보안 전략을 구현하는데 필요한 여러 요소들에 대한 총체적 검토가 부족할 수 있다는 의미로, 보안 담당자가 조직내에 보안을 구현하기 위한 전략을 계획으로 구체화할 때 개인적인 능력이나 경험 등에 따라 누락되거나 간과되는 요소들이 발생할 수 있다는 것을 의미한다.

3.2 정보 시스템 보안 총괄 전략

전통적인 전략에서는 일반적으로 회자되는 전략보다 상위 개념의 전략을 총괄 전략(Grand Strategy)이라 표현한다. 총괄 전략은 '전체 전략(Total Strategy)' 또는 '상위 전략(Higher Strategy)'이라고도 하는데, "정책적 목적 달성을 위하여 국가 또는 여러 국가의 모든 자원을 활용하는 술(術)"을 가리킨다[13](p. 63). Posen[14]은 총괄 전략을 "한 국가가 자국의 안보를 지키기 위한 최선의 방법에 관한 이론"(p. 13)으로 정의하였으며, Reiter and Meek [15]는 여기에 더해 "광범위한 영역의 비군사적인 요소도 포함된다"(p. 367)고 설명하였다. 한편, Layne [16]은 총괄 전략을 "국가의 안보에 관련된 이익이 무엇인지 결정하고, 이 이익에 대한 위협을 식별하며, 이 이익을 지키기 위하여 국가의 정치적, 군사적 및 경제적 자원을 가장 잘 활용할 수 있는 방안을 찾는 것"(p. 88)으로 정의하였다.

이와 같은 여러 정의를 정보 시스템 보안에 적용해 보면, 정보 시스템 보안 총괄 전략은 내·외부의 공격으로부터 조직의 정보 시스템을 보호하기 위하여 조직 전체의 역량을 동원하는 것으로 이해할 수 있다. 즉, 정보 시스템 보안 전략이 보안 수단들을 적절히 배치하고 운영하는 것에 초점이 맞추어져 있다면, 정보 시스템 보안 총괄 전략은 조직의 모든 자원과 구성원을 활용하여 조직의 정보 시스템을 보호하기 위한 종합적인 대안을 제시하는 것이라 할 수 있다. 이러한 측면에서 볼 때, 총괄 전략의 위상은 조직의 비즈니스 전략의 하부 전략인 조직 IT 전략의 하부 전략으로서, 보안 전략 보다는 상위에서 보안에 관련된 조직 전체의 노력을 총괄하는 것으로 정리될 수 있을 것이다.

4. 정보 시스템 보안 총괄 전략 프레임워크

4.1 참조 모델

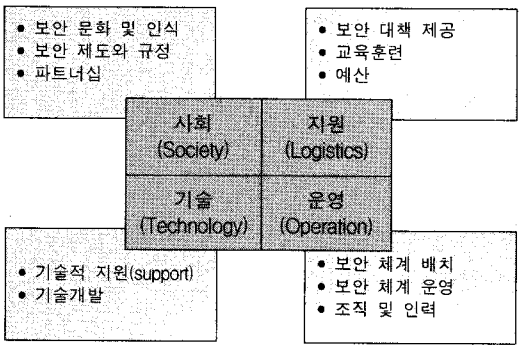
본 연구에서는 조직의 정보 시스템 보안을 위한 총괄 전략 프레임워크를 제시하기 위하여 Howard [17, 18]가 제시한 총괄 전략 모델을 참조하였다. Howard[17, 18]는 공산사회는 마르크스-레닌의 총력전 개념을 바탕으로 하고 있는 반면 서구사회는 군대의 배치와 운영 측면에서만 전략을 바라보다 보니 산업, 경제, 사회 등 여러 측면이 누락되어 있어 이를 포함시키기 위하여 총괄 전략의 개념이 도입되었다고 지적하고, 이 총괄 전략은 사회(Social), 지원(Logistical), 운영(Operational), 그리고 기술(Technological)의 네 가지 차원(Dimension)을 갖는다고 주장하였다. 여기서, 사회 차원은 전쟁에 대한 구성원의 지지 의지를 나타내는 것으로, 애국심이나, 자기 희생과 전쟁 참여 의지 등을 포함한다. 지원 차원은 전장에서 군대의 유지에 관련된 것으로 군대의 양성과 이동 수단의 확보 그리고 필요한 장비를 제공하는 것 등을 다룬다. 그리고 운영 차원은 군사력의 직접적 활용에 관련된 것으로, 군대의 배치와 공격/방어에 관련된 의사결정을 포함하는데, 일반적으로 언급되는 전략의 대부분은 운영 차원의 전략을 의미한다. 마지막으로, 기술 차원은 사용되는 무기에 관한 것으로 무기의 기술적 우수성과 타 차원에 대한 기술적 지원을 다룬다.

4.2 정보 시스템 보안 총괄 전략 프레임워크

앞 절에서 설명한 각 차원은 시대와 상황에 따라 강조되기도 하고 간과되기도 하였다[17]. 전쟁

에서의 승리를 위해서는 전쟁의 목적과 목표, 전장의 상황 등에 따라 다소 강조가 되는 차원과 강조 정도는 달라질 수 있겠지만 네 가지 중 어느 하나도 총괄 전략 수립에 있어서 무시될 수는 없다. 마찬가지로, 조직의 정보 시스템을 보호하기 위한 총괄 전략을 종합적 · 입체적으로 수립하기 위해서는 이 네 차원이 모두 동시에 고려되어야 한다.

본 논문에서는 이 네 차원 모델을 조직의 정보 시스템 보안 총괄 전략에 적용하여 (그림 1)과 같은 프레임워크를 제시한다. 여기서, 사회 차원은 조직의 사회적 측면에서 보안에 관련된 조직의 제도와 분위기와 관련되고, 지원 차원은 보안을 위한 조직 차원의 자원 지원 즉 보안 인력과 보안 대책의 준비와 공급에 관련된다. 또한, 운영 차원은 일선에서 보안 체계를 운영하는 측면에서 보안 체계와 인력/조직의 배치와 적용을, 그리고 기술 차원은 보안 대책의 기술적 사항에 관한 것을 각각 다룬다.



(그림 1) 조직 정보 시스템 보안 총괄 전략 프레임워크

4.2.1 사회 차원

사회 차원에서는 보안에 관련된 조직 문화, 보안에 관련된 제도, 그리고 유관기관과의 파트너십을 다루어야 한다. 먼저, 보안 문화(Security Culture) [56-58]는 아직까지 국내에서는 크게 주목을 받지는 못하고 있지만 선진국에서는 그 중요성이 강조되면서 꾸준히 연구되고 있는 분야로, 조직의 구성원이 보안의 중요성을 인식하고 자발적으로 참여하는 분위기를 형성하고 이러한 인식을 확산시키는 것이다. 과거에는 보안이 보안 임무를 담당하는 소수에게만 한정된 주제였으나, 이제는 비즈니스의 유형이나 부서의 성격과 임무 등에 따라 차이가 있기는 하지만 조직의 전 직원이 관심을 가지고 참여하여야 하는 기본 사항이 되었다. 예를 들어, 모든 직원은 조직의 정책에 따라 컴퓨터의 비밀번호를 정기적으로 변경하여야 하며 지정된 보안 소프트웨어를 설치하여야 하고, 개인적인 차원에서 볼 때는 인터넷 뱅킹을 위한 공인인증서를 사용하여야 하는 등 보안은 우리의 업무와 생활속에 깊숙이 자리를 차지하고 있다. 따라서 보안은 조직내에서 하나의 문화로 자리매김해야 한다. 그리고 이는 인식제고와 홍보를 위한 다양한 프로그램으로 연계되어야 하기 때문에 보안 총괄 전략에서 반드시 다루어야 한다.

다음은 제도와 규정이다. 조직 내에는 보안이 지속적으로 지켜지게 유도하기 위한 제도도 도입되어야 하며 보안을 지키지 않았을 경우를 상정한 제재 방안도 마련되어 있어야 한다. 그리고 각종 제도와 상벌 외에도, 보안을 위한 조직의 기본 방침, 정보 시스템 보안을 위하여 조직 구성원이 하여야 할 일, 보안 조직의 구성, 임무 분장, 책임과 권한의 위임 등이 이행력과 구속력을 갖기 위해서는 규정으로 문서화되어야 한다. 만약 국가적 차원이라면 법의 제정이나 행정명령 등의 형태가 될 수도 있을 것이다. 여기서 추가적으로 고민하여야 할 것은 제도와 규정의 적용 범위이다. 한 조직의 제도와 규정은 조직 내부를 규제하는 것이기 때문에 외부에 대해서는 현실적으로 영향력이 없는 경우가 대부분이다. 하지만, 정보 시스템 보안은 그 특성상 외부로부터의 위협이 많다는 점에서 괴리가 발생하게 되고 조직의 대응이 한계에 부딪히게 된다. 예를 들어, 해커의 불법 침입이 발견된 경우, 내부자의 소행이라면 조직의 제도와 규정에 따라

조사와 처벌 등 적절한 조처를 취할 수 있을 것이다. 하지만 외부로부터의 침입이라면 사법권의 도움없이는 공격자의 신원확인에서부터 조사와 처벌이 거의 불가능할 뿐 아니라, 조직 내부의 규정을 외부인에게 적용하기도 거의 불가능하다. 따라서 외부로부터의 위협을 인지하거나 사고가 발생한 경우, 내부적으로는 사실을 증빙할 수 있는 충분한 증거를 확보하고(경우에 따라 현장 보존이 필요할 수도 있음) 그 내용을 보고하며, 외부적으로는 확보된 증거를 근거로 공권력이 발효되는 사법체계에 의존(예 : 신고, 고소, 고발, 자료협조 등)하는 방향으로 규정이 마련되어야 한다.

정보 시스템 보안은 조직 자체의 노력만으로는 한계가 있는 경우가 많다. 새로운 위협이 지속적으로 등장하고 있고 공격의 전파 속도도 빠르며 상황 역시 시시각각으로 변화하고 있다. 이러한 상황에서는 혼자만의 노력으로는 조직의 정보 인프라를 보호하기 어렵기 때문에 유관기관과의 연계가 필수적이다. 즉, 유사한 비즈니스 분야(예 : IT, 금융 등) 또는 유사한 인프라 환경을 가진 타 기관과 정보 시스템 보안에 관하여 협력관계를 구축하거나 기존 단체의 활동에 참여함으로써 전략적 파트너십을 구축하고, 협력과 공조를 통해 유행하는 위협과 이에 대응하기 위한 대책에 관한 정보와 경험을 공유하여 활용할 수 있어야 한다.

4.2.2 지원 차원

지원 차원에서는 보안 대책의 제공, 교육훈련, 그리고 예산을 다루어야 한다. 먼저, 개인 및 조직에서 보안체계의 구축을 위해 사용할 보안 대책(예 : 방화벽, 침입 탐지 시스템, 메일 필터 등)을 획득하여 보급하여야 한다. 또한, 여기에는 보안 장비나 소프트웨어 등의 보안 대책이 정상적으로 운영될 수 있도록 지원하기 위한 IT 자원의 배분(적정 Bandwidth와 프로세서·메모리 등)도 포함되어야 한다.

다음으로 획득된 각 보안 대책과 구축된 보안 체계에 대한 교육훈련이 다루어져야 한다. 확보된 인력을 조직 전체의 보안을 책임지는 보안 전문 인력으로 양성하고 전문성을 강화하는 내용으로 교육훈련이 추진되어야 한다는 점에는 이견이 없을 것이다. 이와 더불어 조직의 일반 구성원을 대상으로 하는 교육훈련도 병행되어야 한다. 개별 구성원은 자신의 개인용 컴퓨터와 자신의 계정 등을 직접 보호하여야 한다. 따라서 조직에서 결정한 패스워드 생성 원칙, 개인방화벽이나 백신 소프트웨어 등 보안 대책의 설치와 설정 방법 등을 이해하고 숙지하여야 한다.

조직을 정보 시스템 보안 위협으로부터 보호하기 위해서는 예산 지원이 필수적이다. 보안 대책의 획득, 보안 대책을 지원하기 위한 IT 지원 규모, 교육훈련 비용, 유지보수 비용, 보안 수준에 관련된 외부 컨설팅 비용 등을 감안하여 적정 규모의 예산이 지원되어야 한다. 총괄 전략이 조직의 보안 정책 목표를 달성하기 위하여 조직의 상황과 실정에 따라 방향과 주요 과제를 제시한다는 측면에서는 전략 수립시 예산은 간과되기 쉬운 요소이다. 하지만 여러 연구에 따르면 예산은 조직의 정보 시스템 보안 정도와 상관관계가 있으므로[40, 52, 54, 59] 전략 수립시 함께 검토되는 것이 바람직할 것이다. 특히, 예산적 검토없이 전략을 수립하였다가 조직내에 전략을 구현할 때 결국 예산상의 이유로 좌절되지 않기 위해서는 예산도 함께 검토되어야 할 것이다.

4.2.3 운영 차원

운영 차원에서는 보안 체계의 배치와 운영, 그리고 보안 조직 및 인력에 관한 전략을 수립하여야 한다. 보안 체계의 배치는 단순히 어떠한 대책을 어디에 위치시킬 것인가 하는 측면에서 나아가, 조직의 보안 목표와 목적 및 기본 철학에 따라 여러 보안 대책이 잘 활용될 수 있도록 전체적인 보안 아키텍처를 구성하고 체계를 구축하는 관점에서 바라보아야 한다. 즉, 어떠한 보안 대책을 어떠

한 목적으로 어떠한 전략에 따라 어떠한 아키텍처 하에 어느 곳에 위치시켜 어떠한 효과를 거둘 것인가를 결정하여야 한다. 이를 위해서는 그 동안 제시되어 왔던 예방, 봉쇄, 종심 방어, 억지, 기만, 모니터링, 탐지, 복구 등 다양한 전략들[12, 26, 31-35, 37-49]이 활용될 수 있을 것이다.

보안 체계가 구축된 이후에는 보안 대책들이 적절히 배치되었는지, 의도된 대로 동작하는지, 업데이트가 적절히 이루어지고 있는지 등을 지속적으로 점검하는 운영 측면이 간과되지 않아야 한다. 그리고 필요에 따라서는 피드백을 통해 보안 대책을 재배치하거나 전체 체계를 재구성하여야 할 수도 있어야 한다. 또한, 보안 체계를 운영한다는 것은 보안 정책을 결정(예 : 패스워드 교체 주기와 생성 원칙, 접근통제 정책, 시스템 점검 항목과 주기 등) 하고 이 결정에 따라 해당 항목의 값을 적절하게 설정(Configure)하는 것도 포함되어야 한다. 특히, 운영에 있어서 설정이 중요한 이유는 Lampson[44]도 지적한 바와 같이 보안이 취약해지는 이유중의 하나가 설정의 복잡성에 기인하기 때문이다. 이는 일반 소프트웨어뿐 아니라 보안 대책에도 동일하게 적용되는 것으로, 보안 대책의 설정이 부적절하면 보안 대책이 의도한대로 동작하지 않게 될 것이고, 결국에는 보안 대책이 없는 것과 마찬가지의 결과를 가져올 수도 있기 때문이다. 설정은 대응 과정에서도 중요한 역할을 할 수 있는데, 예를 들어 특정 포트를 차단하는 것 등이 이러한 범주에 포함될 수 있다. 그리고 보안 체계를 효과적이고도 체계적으로 운영하고 사고에 적절하고도 긴밀하게 대응하기 위해서는 정보 시스템 보안 체계 운영 매뉴얼을 작성하여 활용하는 것도 필요하다.

보안 총괄 전략을 조직내에 구현하고 동작하게 하기 위해서는 조직과 인력이 필요하다. 따라서 조직 정비와 인력 확보 측면에서, 보안 부서를 어떠한 규모와 구조로 어떠한 지휘체계하에 편성하고, 어떠한 인력을 확보할 것인가, 부서와 인력의 임무와 역할을 무엇인가 등 보안 부서에 대한 검토 역시 운영 차원에서 이루어져야 한다. 특히, 조직과 인력 측면에서는 보안 담당 부서의 위상, 보고 체계, 인력의 전문성 등이 총괄 전략의 효과적 운영 여부를 판가름하게 하는 요소로 작용한다는 점을 간과하지 말아야 한다[40, 52, 54].

4.2.4 기술 차원

기술 차원은 그간 강조되어 왔던 바와는 달리 조직내에서 부각되는 역할이 상대적으로 많지 않다. 그 이유는 대부분의 조직이 보안 대책을 직접 개발하기 보다는 상용 제품을 사용하기 때문일 것이다. 따라서 기술 차원에서는 정보 시스템 보안에 관련된 기술적 사항 그리고 다른 세 차원에서 필요로 하는 기술적 사항에 대하여 지원(support)하는 역할을 정립하여야 한다. 구체적으로 설명하면, 위협을 분석하거나 보안/위협의 동향을 파악하는 것, 또는 보안 대책들을 도입하려 할 때 배치와 운영 전략에 따라 각 대책이 갖추어야 할 기능, 성능 등의 목표와 기준을 작성하고, 기술적 우월성을 판단하는 것 등이 포함된다.

대기업 정도 규모의 큰 조직 또는 국가적 차원이거나, 보안 대책을 자체적으로 개발할 여력이나 현저한 필요성이 있는 경우에는 기술 개발이 중요한 항목이다. 하지만 그렇지 않은 경우에는 직접 개발보다는 구매를 통한 외부 도입을 추진하게 될 것이므로 기술 개발의 상당부분이 축소되고 기술 지원이 강조되어야 할 것이다.

5. 정보 시스템 보안 총괄 전략 프레임워크의 평가

본 연구에서 제시한 프레임워크의 적절성을 검토하기 위하여 2003년 미국에서 발표된 사이버 보안 국가 전략[60]과 동년 발표된 우리나라의 정보보호 종합계획[61]을 활용하였다. 그 이유는 첫째

일반 조직의 총괄 전략을 입수하기 어렵기 때문이다. 둘째 이유는, 국가 차원의 전략이나 종합계획은 총괄 전략에서 다루어야 하는 상위 수준의 사항들을 종합적으로 다룰 것이므로 본 연구에서 제시하는 프레임워크를 점검하기에 적절하다고 판단하였기 때문이다. 특히, 한국의 종합계획은 전략은 아니지만 국가적 차원의 중기계획이므로 추진 일정과 로드맵 등을 제외하면 총괄 전략의 상당한 요소를 포함하고 있을 것으로 판단하여 이를 활용하게 되었다.

미국의 국가 전략[60]에는 미국이 국가 사이버 보안을 위하여 추구해야 할 다섯 가지 핵심 방향이 제시되었는데, 사이버보안 대응 시스템 구축, 사이버위협 및 취약점 감소 프로그램 개발, 사이버 보안 인식제고 및 훈련 프로그램 개발, 정부 사이버공간 보호, 그리고 국제 및 국가 안보 차원의 협력 강화이다. 각 방향에는 여러 가지 세부 방향들이 제시되었는데, 사이버공격의 전술·전략적 분석과 취약점 진단 등 모두 39개 항목이 도출되었다. 한편, 우리나라의 종합계획[61]은 법제 정비, 대응력 제고 및 기반시설 보호 강화, 사회적 환경 및 관행 개선, 안전성 제고, 산업육성 및 전문인력 양성, 그리고 인식제고의 여섯 가지 항목으로 구성되어 있다. 세부 항목은 개인정보보호법 제정 등 모두 40개가 도출되었다.

각 세부 항목이 본 연구에서 제시한 프레임워크의 어느 항목에 해당하는지 종합하면 <표 1>과 같다. 이 때, 미국 국가 전략과 우리나라 종합계획의 세부 항목이 프레임워크 요소 두 개 이상에 해당될 때(예 : 정보 전문가 양성을 위한 장학금 제도 시행)에는 각 요소를 모두 나타내는 것으로 중복 표기하였다. 또한, 본 프레임워크로는 표현할 수 없는 세부 항목이 미국 국가 전략에서 한 개 그리고 우리나라 종합계획에서 두 개가 발견되었다. 미국 국가 전략의 경우에는 적적한 방법을 이용하여 대응할 권리를 확보하는 것(Reserve the Right to Respond in an Appropriate Manner)으로 내용적으로는 외국이나 테러집단으로부터의 사이버공격이 발생할 경우 범죄에 대응하는 측면을 뛰어넘는 다소 적극적 방어의 개념이 포함되어 있어 일반적인 조직에는 적용하기 어려운 내용일 뿐 아니라 본 연구에서 제시하는 정보 시스템 보안 총괄 전략 프레임워크에서도 전혀 고려하고 있지 않은 사안이다. 우리나라 종합계획의 경우에는 해외 마케팅 지원과 정보보호 게임 개발이 본 프레임워크로는 표현할 수 없는 항목에 해당되었다.

이 표를 보면, 미국의 국가 전략은 파트너십의 구축, 보안 체계의 배치, 그리고 기술 지원에 중점을 두고 있는 반면, 우리나라의 종합계획은 제도와 규정을 중점으로 하고 있음을 알 수 있다. 또한, 미국의 국가 전략은 대체적으로 균형을 이룬 가운데, 사회 차원, 운영 차원, 그리고 기술 차원을 고르게 강조하고 있는 한편 지원 차원은 상대적으로 덜 강조하고 있음을 알 수 있다. 반면, 우리나라의 종합계획은 전체적으로 사회 차원에 대한 쏠림 현상이 발생하는 가운데 지원과 운영 차원은 균등하

〈표 1〉 미국 국가 전략과 우리나라 종합계획에 나타난 프레임워크 요소

프레임워크	사회			지원			운영			기술	
	보안 문화	제도 규정	파트너십	대책 구비	교육 훈련	예산	체계 구축	체계 운영	조직 인력	기술 지원	기술 개발
미국 국가 전략	1	3	9	0	3	0	9	4	1	9	4
	13			3			14			13	
우리나라 종합계획	5	15	2	6	5	0	5	2	4	3	1
	22			11			11			4	

게 강조되었으나 기술 차원에 대한 강조는 미약함을 알 수 있다. 두 나라 전략/계획의 공통점으로는, 예산에 관한 내용이 모두 누락되어 있다는 것이다. 그 이유를 분석해보면, 국가 전략이나 종합계획의 실현을 위해서는 비용이 필요함은 분명하지만 예산의 규모, 투입분야, 조달방안 등을 제시하기보다는 예산과 관계없이 전체적인 추진 방향성과 핵심 과제를 식별하는데 초점을 맞추었기 때문으로 판단된다. 그럼에도 불구하고, 조직에서는 총괄 전략을 수립할 때 예산을 제외시키지 말아야 한다. 그 이유는 현재까지 조직의 보안이 항상 부족하고 불충분했던 이유가 바로 비용 투자의 부족에 기인하기 때문이다[44]. 물론, 조직의 보안은 당연히 비용대비 효과적(cost-effective)이어야 하지만[29, 44, 51], 예산은 정보 시스템 보안을 향상하는데 있어서 간과되지 말아야 할 중요한 요소이기 때문이며[52], 나아가 "비용(expense)"이 아닌 "투자(invest)"의 개념으로 전환되어야 하기 때문이다[62]. 결론적으로, 두 나라의 전략과 종합계획을 중심으로 평가하였을 때, 본 연구에서 제시하는 조직 정보 시스템 보안을 위한 총괄 전략 프레임워크가 적절함을 알 수 있다.

6. 결 론

전략은 기업과 군사 분야뿐 아니라, 연구개발, 정책과 계획의 수립 등 다양한 분야에 적용되고 있는 중요한 개념이다. 정보 시스템 보안 분야에도 전략이 도입되어야 하며, 이러한 움직임은 계속 진행되어야 한다. 이를 위해서는 일반적으로 보안 대책의 배치와 운영을 다루는 전략의 상위에서 조직 전체가 참여할 수 있도록 전사적인 전략이 수립되어야 한다.

본 논문에서는 그동안 전략에 관하여 제시되어 왔던 여러 개념 중 총괄 전략이 이에 적합한 것으로 파악하고, 이 개념을 정보 시스템 보안에 적용하여 정보 시스템 보안 총괄 전략의 개념을 정립하였다. 또한, 총괄 전략이 갖는 특성을 설명한 4차원 모델을 기반으로 총괄 전략의 프레임워크를 제시하였으며, 미국과 우리나라의 국가 전략과 종합계획을 활용하여 그 적절성을 분석하였다.

본 연구는 아직까지 학문적으로 시도되지 않았던 것으로서, 조직의 정보 시스템 보호를 위한 전사적 전략 수립에 사용될 프레임워크를 제시하였다는 측면에서 학술적 의의를 갖는다. 본 논문에서 제시된 프레임워크를 사용하면 조직 전체 차원에서 정보 시스템 보안을 위하여 추진해야 할 총괄 전략을 체계적으로 정립할 수 있을 것이다. 또한, 기존 총괄 전략에 대해서도 과도하게 중점을 두고 있는 부분과 간과되고 있는 부분을 발견하여 보완하는데 사용할 수도 있을 것이다. 나아가, 정보 시스템 보안 전략을 조직내에 성공적으로 구현하는데 관련된 요인들을 검토하여 각 조직에 적합하도록 가중치를 조절한다면, 조직의 특성, 환경과 상황에 보다 최적화된 보안 체계를 구축하는데 도움이 될 것으로 판단된다.

참 고 문 헌

[1] B. Chess and G. McGraw, "Static Analysis for Security", IEEE Security and Privacy, Vol. 2, No. 6, pp. 76-79, Nov./Dec. 2004.

[2] J. A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Dec. 2002.

[3] R. Richardson, 2008 CSI Computer Crime and Security Survey, Computer Security Institute, 2008.

[4] FSB, Inhibiting Enterprise: Fraud and Online Crime Against Small Business, Federation of Small Businesses, 2009.

[5] Symantec, Managed Security in the Enterprise (U.S. Enterprise), Symantec, Mar. 2009.
[6] Ernst and Young, Moving Beyond Compliance : Ernst and Young's 2008 Global Information Security Survey, Ernst and Young, 2008.
[7] R. A. Botha and T. G. Gaadingwe, "Reflecting on 20 SEC conferences", Computers and Security, Vol. 25, No. 6, pp. 247-256, 2006.
[8] M. R. Benioff, E. D. Lazowska, et al., Report to the President, Cyber Security : A Crisis of Prioritization, President's Information Technology Advisory Committee (PITAC), Feb. 2005.
[9] S. Landau and M. R. Stytz, "Overview of Cyber Security : A Crisis of Prioritization", IEEE Security and Privacy, Vol. 3, No. 3, pp. 9-11, May/Jun. 2005.
[10] B. V. Solms, "Information Security-The Third Wave?", Computers and Security, Vol. 19, pp. 615-620, 2000.
[11] B. V. Solms, "Information Security-The Fourth Wave", Computers and Security, Vol. 25, pp. 165-168, 2006.
[12] 박상서, "조직 차원의 정보보안전략의 개념", 정보보안논문지, Vol. 7, No. 3, pp. 15-24, Sep. 2007.
[13] R. Evered, "So What is Strategy?", Long Range Planning, Vol. 16, No. 3, pp. 57-72, 1983.
[14] B. R. Posen, The Sources of Military Doctrine : France, Britain, and the Germany Between the World Wars, Ithaca, NY : Cornell University Press, 1984.
[15] D. Reiter and C. Meek, "Determinants of Military Strategy, 1903~1994 : A Quantitative Empirical Test", International Studies Quarterly, Vol. 43, No. 2, pp. 363-387, Jun. 1999.
[16] C. Layne, "From Preponderance to Offshore Balancing : America's Future Grand Strategy", International Security, Vol. 22, No. 1, pp. 86-124, Summer 1997.
[17] M. Howard, "The Forgotten Dimensions of Strategy", Foreign Affairs, Vol. 57, No. 5, pp. 975-986, Summer 1979.
[18] B. Martin, "Social Defense Strategy : The Role of Technology", Journal of Peace Research, Vol. 36, No. 5, pp. 535-552, Sep. 1999.
[19] H. Mintzberg, "Patterns in Strategy Formation", Management Science, Vol. 24, No. 9, pp. 934-948, May 1978.
[20] A. D. Chandler, Strategy and Structure, Cambridge, Massachusetts : MIT Press, 1962.
[21] K. R. Andrews, The Concept of Corporate Strategy, 3rd ed., Homewood, Illinois : Richard D Irwin, 1987.
[22] M. E. Salveson, "The Management of Strategy", Long Range Planning, pp. 19-26, Feb. 1974.
[23] C. V. Clausewitz, On War, Dutton, 1918.
[24] B. H. Linddell-Hart, Strategy, New York : Praeger, 1968.
[25] O. S. Saydjari, "Cyber Defense : Art to Science", Communications of the ACM, Vol. 47, No. 3, pp. 53-57, Mar. 2004.
[26] S. Park and T. Ruighaver, "Strategic Approach to Information Security in Organizations", Proc. of the 2008 IEEE International Conference on Information Science and Security (ICISS 2008), pp. 26-31, Seoul, Korea, 2008.
[27] D. Reiter, "Military Strategy and the Outbreak of International Conflict : Quantitative Empirical Tests, 1903~1992", The Journal of Conflict Resolution, Vol. 43, No. 3, pp. 366-387, Jun. 1999.

[28] W. Agrell, "Offensive versus Defensive : Military Strategy and Alternative Defence", Journal of Peace Research, Vol. 24, No. 1, pp. 75-85, Mar. 1987.

[29] J. Sherwood, "SALSA : A Method for Developing the Enterprise Security Architecture and Strategy", Computers and Security, Vol. 15, pp. 501-506, 1996.

[30] S. Edwards and M. C. Willimas, "The Need for In-Depth Cyber Defence Progrmmes in Business Information Warfare Environments", Proc. of the 2nd Australian Information Warfare and Security Conf. 2001, pp. 56-63, 2001.

[31] T. Grance, K. Kent, and B. Kim, Computer Security Incident Handling Guide, NIST Special Publication 800-61, National Institute of Standards and Technology, Jan. 2004.

[32] P. Mel, K. Kent, and J. Nusbaum, Guide to Malware Incident Prevention and Handling, Recommendations of the National Institute of Standards and Technology, NIST Special Publication (SP) 800-83, National Institute of Standards and Technology, Gaithersburg, MD, Nov. 2005.

[33] S. M. Walt, "The Renaissance of Security Studies", International Studies Quarterly, Vol. 35, No. 2, pp. 211-239, Jun. 1991.

[34] P. Bowen, J. Hash, et al., Information Security Handbook A Guide for Managers, Recommendations of the National Institute of Standards and Technology, NIST Draft Special Publication (SP) 800-100, National Institute of Standards and Technology, Gaithersburg, MD, Jun. 2006.

[35] D. S. Alberts, Defensive Information Warfare, NDU Press Book, National Defense University, 1996.

[36] W. Tirenin and D. Faatz, "A Concept for Strategic Cyber Defense", Proc. of the MILCOM 1999, pp. 458-463, 1999.

[37] L. S. Tinnel, O. S. Saydjari, and D. Farrell, "Cyberwar Strategy and Tactics", Proc. of the 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, pp. 228-234, Jun. 2002.

[38] J. T. Hamill, R. F. Deckro, and J. M. Kloeber Jr., "Evaluating Information Assurance Strategies", Decision Support Systems, Vol. 39, pp. 463-484, 2005.

[39] D. B. Parker, Computer Security Management, Reston, VA : Reston Publishing, 1981.

[40] A. Kankanhalli, H.-H. Teo, et al., "An Integrative Study of Information Systems Security Effectiveness", International Journal of Information Management, Vol. 23, pp. 139-154, 2003.

[41] D. W. Straub, "Effective IS Security : An Empirical Study", Information Systems Research, Vol. 1, No. 3, pp. 255-276, 1990.

[42] K. A. Forcht, Computer Security Management, Danvers, MA : Boyd and Fraser, 1994.

[43] D. W. Straub and R. J. Welke, "Coping with Systems Risk : Security Planning Models for Management Decision Making", MIS Quarterly, Vol. 22, No. 4, pp. 441-469, Dec. 1998.

[44] B. W. Lampson, "Computer Security in the Real World", Computer, Vol. 37, No. 6, pp. 37-46, Jun. 2004.

[45] H. Yang, H. Luo, et al., "Security in Mobile Ad Hoc Networks : Challenges and Solutions", IEEE Wireless Communications, Vol. 11, No. 1, pp. 38-47, Feb. 2004.

[46] D. Armstrong, S. Carter, et al., "Autonomic Defense : Thwarting Automated Attacks via Real-Time Feedback Control", Complexity,

Vol. 9, No. 2, pp. 41-48, 2004.

[47] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Vol. 34, No. 2, pp. 39-53, Apr. 2004.

[48] C. L. Smith, "Understanding Concepts in the Defense in Depth Strategy", Proc. of the IEEE 37th International Carnahan Conference on Security Technology, pp. 8-16, Oct. 2003.

[49] J. Ölnes, "Development of Security Policies", Computers and Security, Vol. 13, No. 8, pp. 628-636, 1994.

[50] S. P. Gorman, R. G. Kulkarni, et al., "Least Effort Strategies for Cybersecurity", Proc. of the The Critical Infrastructure Project Workshop I : Working Papers, pp. 1-14, May 2003.

[51] S. Liu, J. Sullivan, and J. Ormaner, "A Practical Approach to Enterprise IT Security", IEEE IT Professional, Vol. 3, No. 5, pp. 35-42, Sep./Oct. 2001.

[52] J. M. Torres, J. M. Sarriegi, et al., "Managing Information Systems Security : Critical Success Factors and Indicators to Measure Effectiveness", Proc. of the ISC 2006, Vol. LNCS 4176, pp. 530-545, 2006.

[53] J. Reason, Managing the Risk of Organizational Accidents, Hants, UK : Ashgate Publishing Ltd., 1997.

[54] C. C. Wood, "Information Systems Security: Management Success Factors", Computers and Security, Vol. 6, pp. 314-320, 1987.

[55] 박상서, 박춘식, "조직내 정보시스템 보안 전략의 성공적 구현을 위한 정보시스템 보안 전략의 특성", 정보보안논문지, 제8권, 제3호, pp. 101-106, 2008.

[56] P. A. Chia, S. B. Maynard, and A. B. Ruighaver, "Exploring Organisational Security Culture : Developing a Comprehensive Research Model", Proc. of the IS ONE World Conference, Las Vegas, NV, USA, Apr. 2002.

[57] OECD, OECD Guidelines for the Security of Information Systems and Networks : Towards a Culture of Security, OECD, Paris, France, July 2002.

[58] A. B. Ruighaver, S. B. Maynard, and S. Chang, "Organisational Security Culture : Extending the End-user Perspective", Computers and Security, Vol. 26, pp. 56-62, 2007.

[59] L. Raymond, "Organizational Context and Information Systems Success : A Contingency Approach", Journal of Management Information Systems, Vol. 6, No. 4, pp. 5-20, 1990.

[60] The White House, The National Strategy to Secure Cyberspace, The White House, Washington, D. C., 2003.

[61] 행정안전부, 정보보호 중기 종합계획, 행정안전부, 서울, 2003.

[62] R. A. Caralli, The Critical Success Factor Method : Establishing a Foundation for Enterprise Security Management, CMU/SEI-2004-TR-010, ESC-TR-2004-010, Carnegie Mellon University, Pittsburgh, PA, Jul. 2004.

박 상 서

1991년 중앙대학교 전자계산학과(공학사)
1993년 중앙대학교대학원 전자계산학과(공학석사)
1996년 중앙대학교대학원 컴퓨터공학과(공학박사)
1996년~1998년 국방정보체계연구소 선임연구원
1998년~1999년 국방과학연구소 선임연구원
2000년~현재 ETRI 부설연구소 책임연구원