조직 차원의 정보보안 전략의 개념

박 상 서*

요 약

정보보안의 중요성에 관한 인식이 증가함에 따라 다양한 보안대책이 조직에 도입되고 있다. 하지만 대부분의 경우 이들 보안대책은 전략적으로 운영되지 않고 있다. 따라서 본 논문은 조직에서의 정보보안 전략은 무엇인가에 대해 개념적으로 연구한다. 이를 위하여 다양한 문헌에서 정보보안 전략이 어떻게 소개되었으며, 어떠한 전략이 제시되어 왔는지 연구한다. 본 논문은 조직의 정보보안에 있어서의 전략 자체에 초점을 맞추어, 개념을 정립하고, 지금까지 제시되어 온 다양한 전략을 식별하여 체계적으로 분류하였다는데 의의가 있다.

Concept of Strategy in Organizational Information Security

Sangseo Park*

ABSTRACT

As the importance of information security increases, organizations are employing various security countermeasures into their information systems. However, they are not being adapted based on a strategic framework. Therefore this paper researches on the concept of the strategy in organizational information security. This paper studies literatures to find out how information security strategies have been discussed and what types of them have been proposed until now. This paper contributes to the formation of concept of strategy and classification of them by focusing on strategies themselves in organizational information security.

Key words : Information Security Strategy, Prevention, Deterrence, Defense-in-Depth, Reaction, Observation, Determination, Activation

* ETRI 부설연구소

1. 서 론

정부뿐 아니라 거의 모든 기업에 있어서 정보기술이 조직(organization)의 생산성과 경쟁력의 원동력으로 자리매김하면서 조직 차원의 정보보안 중요성은 점차 증가하고 있다. 하지만 보안 취약점과 문제점들은 IT 제품과 기술뿐 아니라 심지어는 보안 제품과 패치에서도 계속적으로 발견되고 있다[1]. 이에 따라 많은 조직들이 보안을 개선하기 위하여 노력을 기울여 왔음에도 불구하고 보안 사고는 줄어들지 않고 있다. 특히, 날이 갈수록 공격 도구들이 지능화 자동화되고 있는 것에 반해[2], 조직에서는 보안대책(security measure)의 단편적인 도입과 운용에 치중하고 있는 실정이다[3]. 더구나 아직까지도 보안이 조직에 완전히 정착되어 있지 않은 상태에서[4] 각 조직에서는 새로운 정보기술을 속속 도입하고 있어, 그렇지 않아도 근본적으로 복잡한 속성을 갖는 보안의 복잡성이 더욱 가중되면서[5, 6] 조직의 보안을 더욱 어렵게 하고 있다.

이와 같은 문제점을 해결하기 위해서는 조직의 정보보안에도 전략의 개념이 도입되어야 하며[3, 7-12], 조직의 전략에도 통합되어야 한다[13]. 그리고 이 전략에 기반하여 조직의 보안 서비스가 정의되고, 보안 메커니즘이 구현되고, 보안 제품이 도입되어야 하며, 나아가 전략이 일상적인 보안 활동에도 직접적으로 영향을 미칠 수 있어야 한다[3, 12].

하지만, 대부분의 조직은 보안전략의 개발을 간과해왔다[12]. 더군다나 몇몇 권고안을 제외하고는 대부분의 조직이 관심을 가지고 있는 표준, 지침서 또는 권고안들에서는 정보보안 전략을 다루고 있지 않다. 게다가 정보보안 전략은 최근 들어 정보보안의 제 4물결[14]에서 하나의 위상을 차지하는 것으로 인식되기 시작할 뿐[15], 아직까지도 정보보안은 기술적 관점에서 주로 논의되고 있는 실정이다[16, 17].

따라서 본 논문에서는 정보보안 전략이란 무엇인가에 대하여 개념적으로 연구한다. 본 논문에서는 정보보안 전략의 개념을 정립하기 위하여 정보보안뿐 아니라 군사와 경영 분야의 문헌으로부터 전략을 무엇이라 기술하였는지 연구하며, 정보보안 및 정보전 분야의 문헌들을 통해 어떠한 전략들이 제시되어 왔는지 연구한다.

본 논문은 크게 두 부분으로 구성된다. 먼저, 전반부에서는 군사와 경영 분야를 중심으로 전략의 일반적인 개념을 살펴보고, 이를 근간으로 정보보안에서 논의되어 왔던 전략의 개념을 분석하여 조직차원의 정보보안에서 적합한 전략의 개념을 정립한다. 후반부에서는, 정보보안 전략을 체계적으로 분류하기 위한 프레임워크를 제안한다.

2. 전략의 이해

전략이라는 용어는 군대의 사령관(a general in command of an army)이라는 의미의 그리이스어 strategos와 10명의 장군들로 구성된 의사결정기구(board of 10 generals)라는 의미의 strategia에서 유래했다[18]. 전략은 초기에는 "장군으로서의 역할(role)"을 의미하였으나 이후, 심리적·행동적 측면에서의 노련미를 의미하는 "장군으로서의 책략(art)"으로 변화하였다. 이후, BC 450년경에는 정치적·국가적 사안에 대한 관리, 통솔, 운영 및 권력의 경영 기술이라는 의미로 사용되었고, BC 330년경에는 군사적 측면에서의 군대 운영 기술을 의미하는 용어로 사용되었다.

전략에 관하여 가장 많은 연구가 진행되어 온 분야는 군사와 경영이다. 이들 분야에서 주장하는 전략의 공통점과 차이점을 살펴보면[18-21], 공통적으로는 전략은 어떠한 "목적"을 달성하기 위하여 "계획"을 수립하고 "행동"을 취하는 것을 의미한다. 하지만 경영의 측면에서는 "what"의 측면 즉 목적이나 목표를 설정하는 것이 중요한 것으로 강조되는 반면, 군사 측면에서는 "how"의 측면이 강조되어 목적을 어떻게 달성할 것인가 즉, 어떠한 수단을 어떻게 활용할 것인가가 주된 관심사이다. 또한, 전략은 완성이라는 개념이 없이 계속적인 변

화를 추구하며 실증적 측면이 강해 실천계획에 따라 반복적으로 생각하고 행동하게 한다. 특히, 전략은 무엇을 할 것인가와 왜 해야 하는가에 관한 문제를 의사결정 패턴, 상황 그리고 조직 전체의 측면에서 다룬다. 또한, 행동에 있어서는 조직적이면서도 상호교환적인(interactive)면을 중시하며 이때 응집력을 강조한다. 또한, 미래에 대비하여 자원의 유동성도 함께 추구하는 특성을 갖는다.

전략과 밀접한 두 가지 개념이 전술(tactics)과 대전략(grand strategy)이다. 전통적으로 전략은 광범위한 공간에서 오랜 기간에 걸쳐 대규모 군대를 배치하는 군사력의 방향을 의미하는 반면, 전술은 전략의 일환으로서 특정한 목적을 달성하기 위하여 전투에서 적은 단위의 부대를 이용하는 소규모 행동 또는 즉각적인 군사력의 적용을 의미한다[19, 22, 23]. 한편, 대전략은 전략의 상위개념으로서 전체전략(total strategy) 또는 상위전략(higher strategy)이라고도 하며, 비군사적인 자원을 포함한 국가의 모든 자원을 이용하여 국가의 정치적 목적을 달성하거나 국가의 안보를 지키고자 하는 일련의 과정을 의미한다[18, 24].

3. 정보보안 전략의 개념

보안에 필요한 자원(대책, 기술, 인력 등)을 무제한 투입함으로써 보안을 달성하는 것은 누구에게나 가능하다. 하지만, 자원이란 것은 항상 제한되어 있기 마련이기 때문에 최소한의 노력과 비용으로 최대한의 효과를 내기 위해서는 전략이 반드시 필요하다. 다시 말해서, 전략 없이는 최소한의 노력과 비용으로 현존하는 보안대책을 어떻게 최대한 활용할 것인지 정립되지 않을 것이고 그 결과 보안대책이 효율적으로 운용되지 못한다. 그럼에도 불구하고 보안에서의 전략은 아직까지도 그 개념이 명확하게 정의되어 있지 않을 뿐더러, 이에 관한 논의도 많지 않은 실정이다. 따라서 본 논문에서는 우선적으로 정보보안에서의 전략의 개념에 관해 먼저 논의하고자 한다.

전략은 근본적으로 생존을 위하여 현재의 상황을 어떻게 타개해나갈 것인지 고민하는 것이라 할 수 있다. 하지만, 경영 측면에서는 주로 경쟁에서의 생존이 화두인 반면 군사적인 측면에서는 갈등에서의 생존이 주된 관심사라는 근본적인 차이점을 발견할 수 있다. 이런 측면에서 볼 때, 정보보안은 내·외부로부터 공격, 위협이나 시도로부터 자신의 정보인프라를 지키는 것을 목표로 하기 때문에, 정보보안에서는 경쟁에서의 생존보다는 갈등에서의 생존이 더 중요한 가치가 된다고 판단된다. 따라서 정보보안 전략은 비록 군사적인 분야에 속하지는 않지만 경영보다는 군사적인 측면에서 접근하는 것이 더 적합하다고 말할 수 있다. 또 다른 이유는, 경영과 군사적 측면에서의 전략의 차이점 측면에서 보면, 정보보안에서 다루어지고 있는 대부분의 주제는 보안의 목표를 설정하는 것보다는[1] 어떻게 보안을 달성할 것인가 하는 것이므로 정보보안 전략은 개념적으로는 경영 측면보다는 군사적인 측면에서 바라보아야 할 것이다.

그렇다면, 군사적 측면에서 볼 때, 전략은 크게 공세적인 전략과 방어적인 전략으로 구분될 수 있다. Reiter[24]는 공세적 전략은 "적을 제거하고 적군을 파괴"(p. 369)하는 것을 목적으로 하고, 방어적 전략은 "적이 의도하는 바를 달성하지 못하도록 하는 것"(p. 369)이라 정의하였다. 여기서 우리는 조직차원의 정보보안 전략이 방어적이어야 하는 근본적인 이유를 찾을 수 있다. 즉, 정보보안은 타 조직의 정보인프라를 파괴 또는 무력화시키는 것이 목적이 아니라, 인터넷이나 네트워크에 연결됨에 따라 내·외부로부터의 공격에 기본적으로 노출되어 있는 자신의 정보인프라를 보호하는 것이 목적이기 때문이다. 따라서 정보보안 전략은

1) 일반적으로 정보보안의 목표는 이미 주어져 있는 상태이다.

근본적으로 방어적이어야 한다.

여기서, 방어적이라는 의미는 순수한 방어이어야 한다는 것이다. 다시 말해, 방어를 목적으로 하나 공세적 개념이 포함되어 있는 전략, 예를 들어 선제공격(strike-first)이나 보복공격(strike-back) 등과 같은 것은 기업차원의 정보보안 전략에서는 다루지 않는다. 따라서 조직 차원의 정보보안 전략은 기본적으로 방어적 방어이어야 하며, 별도로 언급하지 않는 한 본 논문에서는 방어적 방어의 의미로 사용한다.

Howard[25]는 방어에는 군수(logistical), 운영(operational), 사회(social) 그리고 기술(technological)의 네 가지 차원(dimension)이 존재하는데, 군수 차원은 군대의 유지에, 운영 차원은 군대의 사용과 의사결정에, 사회 차원은 구성원의 의지에, 그리고 기술 차원은 무기와 타 차원의 지원에 각각 관련이 있다고 언급하였다. 이를 정보보안에 적용하면, 군수 차원은 보안 인력의 훈련과 보안대책의 공급, 운영 차원은 어떠한 보안대책을 사용할 것인지 결정하고 해당 보안대책의 적용, 사회 차원은 조직 구성원의 보안 의식 함양, 그리고 기술 차원은 공격·위협의 분석이나 보안 도구의 세팅 등으로 표현될 수 있을 것이다. 따라서 보안 전략은 이들 네 차원 중 운영의 차원에서 다루어져야 한다. 즉, 정보보안 전략은 내외부의 정보보안 위협으로부터 정보인프라를 보호함으로써 기밀성, 무결성 그리고 가용성을 제공하기 위하여 방어적 방어 측면에서 어떠한 보안대책을 어떻게 사용할 것인지 결정하고 이에 따라 적절한 보안대책을 배치·적용하는 것이다. 한편, 이 네 차원 모두를 다루는 것은 정보보안 대전략이라 할 수 있을 것이다.

4. 정보보안 전략의 필요성

4.1 보안대책의 효과적 운용

우선, 적절한 수단을 효과적으로 사용하기 위하여 필요하다. 탁월한 능력을 가진 보안제품이나 뛰어난 기술이 있더라도 적절한 전략에 기초하여 활용하지 않으면 효과를 충분히 발휘하기 어렵다. 하지만 전략을 사용하면 제한된 보안 자원중에서 적절한 수단을 선별하여 최대한 효과적으로 활용할 수 있다[20, 26, 27]. 특히, 전략을 사용하면 보다 체계적으로(structured), 조직적으로(organized) 그리고 준비된(prepared) 상태에서 보안위협에 대처할 수 있다. 한 두 가지 대처방식을 독립적으로 사용해서는 최근의 보안위협을 방어하기 어렵기 때문에, 여러 보안대책을 적절히 혼용하거나(mixture) 조화시켜(coordinate) 적용하고, 효과적으로 운용할 수 있는 전략이 필요하다[3, 6, 11]. 게다가 어떠한 전략을 어떻게 개발하고 운용하느냐에 따라 약점이 감추어지기도 하고, 약점이 장점으로 바뀌기도 하며, 강점이 배가되기도 한다.

4.2 한 두 보안대책의 실패하더라도 피해와 파급효과 축소

보안에 관하여 지속적으로 강조가 되고 있음에도 불구하고 내재되어 있는 소프트웨어적 취약성 때문에 대부분의 컴퓨터는 아직까지도 안전하지 않은 것으로 알려져 있다[28]. 그리고 이러한 문제가 전격적으로 해결되지도 못하고 있다 보니 새로운 정보기술을 도입하는 것 자체가 새로운 보안위협이 되고 있다[29]. 또한, 보안위협기술 역시 발전하기 때문에 이에 대처하기 위한 보안기술도 점점 복잡해져 더 많은 위험요인을 제공하고 있으며 심지어는 보안대책을 설정하고 잘 활용하는 것조차 어려워지고 있다[30, 31]. 그뿐 아니라, 위협을 감소시키고 피해를 국지화시키기 위한 목적으로 여러 이기종 시스템을 사용하는 경우도 있어[31] 보안 자체의 복잡성은 지속적인 증가일로에 있다[32].

이러한 상황에서는 보안대책이 효과를 발휘하기도 어렵고 실패할 가능성도 높을 뿐 아니라, 현재 적용중인 보안대책이 실패하였는지 인지하여

적절히 대처하기도 어려울 수 밖에 없다. 그렇다고 정보기술의 활용을 최대화하기 위하여 보안대책을 적용하지 않을 수도 없다. 따라서 정보기술의 활용성(usability)과 보안성 사이의 균형을 유지하는 것도 중요하지만[33], 적용중인 보안대책이 실패하더라도 그 피해와 파급효과를 줄이고, 적절한 대처가 가능하도록 대비하기 위해서는 전략의 개발이 반드시 필요하다.

4.3 고도화된 위협에 유연하게 대처

또한, 위협의 고도화(sophistication of threats)에 적절하게 대처하기 위하여 필요하다. 최근의 보안위협, 보안공격, 그리고 공격도구들은 점차 고도화, 자동화, 지능화, 강화되고 있다[2, 6, 34]. 공격자들은 보안대책을 회피하거나 무력화시키기 위한 방안들을 고안하고 있고, 언더그라운드에서는 이러한 정보들이 교환되고 있다. 게다가 그들은 점차 전략적 공격 목표를 설정하여 겨냥하기 시작했으며, 그 동기도 단순한 호기심을 넘어 범죄와 금전적 이득으로 변화하고 있다. 더구나 Zero-Day attack 앞에서는 정보인프라가 고스란히 위협에 노출되어 속수무책으로 피해를 당할 수 밖에 없는 실정이다. 이는 현존하는 보안대책을 단순히 운영하는 것만으로는 보안대책이 더 이상 유효하지 않으며, 조직의 정보인프라는 더 이상 안전하지 않다는 의미이다. 그렇다고 해서 현재의 정보인프라와 보안대책을 완전히 무시하고 처음부터 완벽에 가까운 보안인프라를 구축할 수도 없는 것이 현실이다. 즉, 현재의 여러 상황과 환경을 이해하고 이를 바탕으로 최적의 효과를 발휘할 수 있는 유연한 방안을 찾아내자는 것이 바로 전략을 필요로 하는 이유이다.

4.4 정보보안의 불완전성을 극복

정보보안은 그 자체가 불완전(imperfect)하여, 내재적으로 불완전성(incompleteness), 비대칭성(asymmetry), 역동성(dynamicity) 그리고 불확실성(uncertainty)의 특성을 갖는다. 완벽한 보안은 불가능하다[35]. 보안 서비스가 기술적으로는 완벽하다고 하더라도 보안의 완벽성에 영향을 주는 여러 요소(예를 들어, 관리의 문제, 사람의 개입, 다른 보안도구와의 상호작용, 도구・서비스의 세팅, 운영되는 기반시스템이 가지고 있는 취약성 등)가 있기 때문이다. 심지어는 보안대책으로부터 새로운 종류의 보안 위험이 전래되기도 한다[5].

정보보안에서 공격자는 방어자에 비해 주로 우위에 있다[26, 36]. 공격자는 한 두 가지 취약점이나 보안결함만이 있어도 정보인프라에 대한 공격을 시작할 수 있는 반면, 방어자는 모든 취약점을 보완하고 모든 예상 공격 경로를 봉쇄해야 한다. 이러한 비대칭적인 상황에서는 많은 보안도구와 보안기법이 사용되어야 하기 때문에 전략적 접근에 기초하여 이들 보안자원을 적절하고 조화롭게 활용하여야 한다.

정보보안은 동적(dynamic)이다. 공격과 상황은 시시각각으로 변화하기 때문에 정보보안 역시 이에 따라 적절히 변화하여야 한다. 즉, 정적인 보안에 집중하는 것은 의미가 없다. 전략은 상황의 변화에 따라 정보보안이 계속 진화할 수 있도록 도와준다. 전략을 활용할 경우 정보보안은 비로소 고도의 책략(術, art)이 된다[6].

이외에도 정보보안에는 불확실성이 존재한다. 즉, 정보인프라가 공격에 노출되어 있으며 이에 대비하기 위하여 보안대책을 적용하고 있다는 것 이외에는 누가 공격을 준비하는지, 정보인프라가 공격을 받고 있는지, 공격을 받고 있다면 언제・어디서부터 공격이 시작되었는지, 공격의 목표와 목적은 무엇인지 등에 대해 명확하게 답변하기 어렵다. 하지만 전략을 도입하게 되면 이러한 불확실한 상황에서도 보안위협에 대처할 수 있는 체계적인 대책을 보유하게 되는 것이다.

5. 정보보안 전략의 분류

정보보안 전략은 <표 1>과 같이 연구자의 관점에 따라 여러 가지로 분류되어 왔다. Straub and Welke[37]는 Straub[7]의 기존 연구 결과를 보완하여 억제, 예방, 탐지 및 치료로 확대하였다. Yang et al.[38]은 선행적 전략은 암호 기술을 이용하는 것이며, 반응적 전략은 탐지와 반응(react)으로 구성된다고 설명하고 있으며, Armstrong et al.[39]과 Mirkovic and Eeiher[40]는 반응적 전략은 공격을 탐지하여 대응(response)하는 것이라고 기술하고 있다.

〈표 1〉 기존의 정보보안 전략 분류

분류	제안자
Deterrence, Prevention	Parker[41], Kankanhalli[8], Straub[7], Forcht[42]
Deterrence, Prevention, Detection, Remedy	Straub and Welke[37]
Isolate, Exclude, Restrict, Recover, Punish	Lampson[31]
Proactive, Reactive	Yang et al.[38]
Preventive, Reactive	Armstrong et al.[39] Mirkovic and Eeiher[40]
Deterrence, Detection, Delay, Response	Smith[43]
Prevention, Limitation, Correction	Olnes[5]

이와 같이 정보보안 전략은 아직까지 체계적으로 분류되지 못하고 있다. 하지만 본 연구에서는 현재까지 제안되어 온 다양한 전략들을 종합적으로 검토한 결과, 전략은 <표 2>와 같이 세 개의 차원 즉 전략의 적용 시기, 전략의 적용 지점, 그리고 전략의 적용을 위한 의사결정 프로세스의 차원에서 분류될 수 있음을 발견하였다.

〈표 2〉 정보보안 전략의 분류 프레임워크

Dimension	Category	
전략의 적용 시기	Proactive	Prevention
		Deterrence
	Reactive	Reaction
전략의 적용 지점	Bordered	Perimeter Defense
	Layered	Defense-in-Depth
전략의 적용을 위한 의사결정 프로세스	Cognitive	Observation
	Determinative	Determination
	Directive	Activation

5.1 차원 1 : 전략의 적용 시기

보안위협 또는 공격이 발생하기 이전에 전략을 적용할 것인지 아니면 위협이나 공격이 현실화되었을 경우 적용할 것인지에 따라 Proactive 전략과 Reactive 전략으로 구분될 수 있고, Proactive 전략은 다시 Prevention과 Deterrence로 구분될 수 있다. Prevention[7, 8]은 사전에 주의를 기울이는 것(precautionary)으로, 공격이 발생하기 이전에 위험을 감소시키고 사전에 피해를 차단하는 것을 목적으로 한다. Deterrence[7, 8, 26, 44]는 방어의 최전선으로 여겨지며, 정보보안에 적용되었을 때 효과적인 것으로 연구되었다. 이 전략의 가장 큰 특징은 보복공격(strike-back)과 같은 징벌(punishment)이 반드시 수반되어야 효과적이라는 것이다. 하지만, 사이버공간에서는 방어측이 외부의 공격자들을 직접적으로 징벌을 하기가 어렵다는 단점이 있다. 게다가 앞에서 설명한 바와 같이 정보보안은 방어적 방어이어야 하기 때문에 실제적으로 이 전략을 정보보안에 그대로 적용하기에는 어려움이 있다.

Reaction[6]은 정보보안 전략에 있어서 필수적인 것으로, 공격이 발생한 경우 피해를 줄이고 공격과 위협에 대응(respond)하기 위하여 적절한 행동(action)을 취하는 것이다. 특히 반응은 정보보

안이 가지고 있는 여러 특성 중 동적 특성을 가장 잘 나타낸다.

5.2 차원 2 : 전략의 적용 지점

전략을 어떠한 지점에 적용할 것인가에 따라 Bordered 전략과 Layered 전략으로 구분된다. 먼저, Perimeter Defense[35]는 조직의 내부와 외부가 구분되는 경계선에 보안대책을 적용하는 것으로, 방화벽이나 접근통제 메커니즘, 사용자 인증장치 등이 대표적인 예이다. 이 전략은 일단 방어선이 무너지면 내부가 공격에 직접 노출되어 막대한 피해를 입게 될 뿐 아니라 더 이상의 방어가 불가능하다는 큰 단점이 있다.

이와 같은 단점을 보완하기 위하여 대두된 방어의 개념이 Defense-in-Depth[3, 26, 45, 46]이다. 즉, 중요한 방어지점마다 각기 다른 유형의 보안 전략을 조합하여 적용하는 다중 방어선을 계층적으로 구성하자는 것이다. 이렇게 함으로써 하나 또는 몇 개의 방어선이 무너지더라도 핵심 정보자산을 보호함과 동시에 정보자산의 운영성을 보장할 수 있다.

5.3 차원 3 : 전략의 적용을 위한 의사결정 프로세스

제 3장에서도 지적한 바와 같이 정보보안 전략은 운영적 차원 즉, 의사결정과 행동의 측면에서 다루어져야 한다. 그러나 지금까지 제안되어 온 여러 분류에서는 전략을 행동으로 옮기는 관점에서 주로 다루고 있을 뿐 의사결정에 관련되어서는 거의 다루지 않고 있다. 그럼에도 불구하고 실제로는 의사결정 프로세스에 관련된 여러 유형의 전략이 제시되어 온 것 또한 사실이다. 따라서 본 연구에서는 이에 관련된 전략들을 하나의 차원으로 이해하고 세부적으로 분류해 내고자 한다.

의사결정에 관련되어 가장 보편적으로 참고 되는 프로세스는 OODA(Observe, Orient, Decide, Act) 모델[47]로, 정보를 입수·분석하고, 결정을 내리고, 그 결정에 따라 적절한 활동을 하는 것으로 정리될 수 있다. 하지만, 여기서의 활동은 의사결정 결과를 직접 수행하는 것이 아니라 의사결정 결과가 효력을 발휘하도록 지시하는 것이어야 한다. (예를 들어, 방화벽 설정을 변경하는 것으로 결정되면, 방화벽 또는 관리 시스템의 설정을 변경하도록 지시하는 것이지 직접 설정을 변경하는 것이 아니다.) 따라서, 의사결정 프로세스 차원에서의 전략은 인지, 결심, 지시의 세 가지 측면으로 세분화될 수 있다.

먼저 Cognitive[48]는 공격자의 행동을 지속적으로 관찰하고 분석하여 공격자의 의도를 파악하고 상황을 이해하는 것이고, Determinative는 공격자에 대하여 방어측이 어떠한 행동을 할 것인지 결심하는 것이다. 그리고 의사결정 결과는 보안자원에 전파되어 각 보안대책에 적용된다.

6. 결 론

전략은 전쟁뿐 아니라 국제·국가관계와 기업의 경영에 있어서도 중요한 역할을 해왔다. 보안도 예외는 아니다. 그 동안 보안은 중요하다고 믿어져 왔고, 조직은 보안을 향상시키기 위하여 많은 노력을 기울여 왔다. 그럼에도 불구하고 현존하는 몇 가지 대책을 단순히 적용하는 것만으로는 현재뿐 아니라 미래의 보안을 유지하기 어려워지고 있다. 그렇다고 해서 보안을 무시할 수 있는 것도 아니며, 전체 보안을 혁신적으로 향상시킬 수 있는 기술이나 제품이 개발되는 것도 아니다. 따라서 가장 적절하고 효과적인 방법은 조직의 특성, 브랜드 가치, 보호해야 할 정보의 가치, 정보보안 인력·기술·제품, 조직 문화, 이 조직에 관심을 갖는 적대적인 사람이나 조직 등 여러 상황을 종합적으로 고려한 전략을 개발하여 적용하여야 한다.

보안에도 전략을 도입하여야 한다는 주장이 전혀 없었던 것은 아니다. 하지만, 이러한 논의가 많지 않아, 그 개념이 아직 정립되지도 않았을 뿐더러, 적용가능한 전략들이 종합적으로 정리되어 있지도 않았다. 따라서, 본 논문에서는 "조직차원의 정보보안 전략이란 무엇인가?" 그리고 "전략들이 어떻게 분류될 수 있는가?"라는 두 가지 질문에 대한 답을 찾고자 문헌 연구를 하였다.

연구 결과, 조직 정보보안에서의 전략은 정보보안 위협으로부터 조직의 정보인프라를 방어하기 위하여 어떠한 보안대책을 어떻게 사용할 것인지 결정하고 이에 따라 적절한 보안대책을 배치·운영하는 것임을 알 수 있었다. 그리고 전략의 적용 시기, 지점, 의사결정 프로세스에 따라 3개의 차원에 걸쳐 8개 카테고리로 구분되는 정보보안 전략 분류 프레임워크를 제안하였다. 본 연구를 진행하며, 여러 연구를 다양한 전략들이 단발적으로 제시되기만 하였지 전체적인 맥락에서 각 전략들을 어떻게 종합적·체계적으로 적용·운용하여야 하는지에 대한 고민은 없었음을 알 수 있었고, 이 문제의 해결 방법은 전략의 구조(architecture of strategies) 측면에서 접근할 수 있다고 판단하게 되었다.

본 연구는 조직차원의 정보보안에서 전략의 개념을 정립하였으며, 전략을 분류하기 위한 프레임워크를 제시하였다는데 의의가 있다. 하지만 본 논문의 한계점은 어떠한 조직이 어떠한 전략을 활용하고 있는지에 관한 실증적 연구가 부족하다는 점이다.

본 논문의 연구 결과를 발전시킴으로써 실제 조직에서 적용 가능한 실용적인 결과를 구조적 측면에서 도출하기 위해서는 ① 조직에서 실제로 어떠한 전략을 사용하고 있거나 사용하지 않는지, 그 이유는 무엇인지, ② 전략의 어떠한 요인들이 해당 전략을 조직내에 효과적으로 구현하는데 영향을 주는지, ③ 이들 요소를 조직의 정보보안 전략 구조 정립하는데 어떻게 활용할 수 있는지에 관한 연구가 필요할 것으로 생각된다.

참 고 문 헌

[1] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) - The Experts Consensus, Version 6.0", SANS Institute, Nov. 2005.

[2] B. Schneier, "Attack Trends 2004 and 2005", QUEUE, pp. 2-3, 2005.

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

[4] "Global Information Security Survey 2005 : Report on the Widening Gap", Ernst & Young, 2005.

[5] J. Olnes, "Development of Security Policies", Computers and Security, Vol. 13, pp. 628-636, 1994.

[6] O. S. Saydjari, "Cyber Defense : Art to Science", Communications of the ACM, Vol. 47, pp. 53-57, 2004.

[7] D. W. Straub, "Effective IS Security : An Empirical Study", Information Systems Research, Vol. 1, pp. 255-276, 1990.

[8] A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei, "An Integrated Study of Information Systems Security Effectiveness", International Journal of Information Management, vol. 23, pp. 139-154, 2003.

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

[10] P. Mel, K. Kent, and J. Nusbaum, "Guide to Malware Incident Prevention and Handling", National Institute of Standards and Technology, Gaithersburg, MD 800-83, Nov. 2005.

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

[12] S. Edwards and M. C. Willimas, "The Need for In-Depth Cyber Defence Progrmmes in Business Information Warfare Environments", presented at 2nd Australian Information Warfare and Security Conf. 2001, 2001.

[13] P. Bowen, J. Hash, M. Wilson, N. Bartol, and G. Jamaldinian, "Information Security Handbook A Guide for Managers(Draft)", National Institute of Standards and Technology, Gaithersburg, MD 800-100, Jun. 2006.

[14] B. V. Solms, "Information Security. The Fourth Wave", Computers and Security, Vol. 25, pp. 165-168, 2006.

[15] T. Tan and A. B. Ruighaver, "Understanding the Scope of Strategic Context in Security Governance", presented at IT Audit : A Strategic Foundation for Corporate Governance, Auckland, New Zealand, 2005.

[16] S. Landau and M. R. Stytz, "Overview of Cyber Security : A Crisis of Prioritization", IEEE Security & Privacy, Vol. 3, pp. 9-11, 2005.

[17] R. A. Botha and T. G. Gaadingwe, "Eflecting on 20 SEC conferences", Computers and Security, Vol. 25, pp. 247-256, 2006.

[18] R. Evered, "So What is Strategy?", Long Range Planning, Vol. 16, pp. 57-72, 1983.

[19] M. E. Salveson, "The Management of Strategy", Long Range Planning, pp. 19-26, 1974.

[20] R. K. Betts, "Is Strategy an Illusion?", International Security, Vol. 25, pp. 5-50, 2000.

[21] H. Mintzberg, "Patterns in Strategy Formation", Management Science, Vol. 24, pp. 934-948, 1978.

[22] C. Edwards and J. Peppard, "Operationalizing Strategy Through Process", Long Range Planning, Vol. 30, pp. 753-767, 1997.

[23] D. Reiter and C. Meek, "Determinants of Military Strategy, 1903-1994 : A Quantitative Empirical Test", International Studies Quarterly, Vol. 43, pp. 363-387, 1999.

[24] D. Reiter, "Military Strategy and the Outbreak of International Conflict : Quantitative Empirical Tests, 1903-1992", The Journal of Conflict Resolution, Vol. 43, pp. 366-387, 1999.

[25] M. Howard, "The Forgotten Dimensions of Strategy", Foreign Affairs, Vol. 57, pp. 975-986, 1978~1979.

[26] W. Tirenin, "A Concept for Strategic Cyber Defense", presented at MILCOM 1999, 1999.

[27] L. S. Tinnel, O. S. Saydjari, and D. Farrell, "Cyberwar Strategy and Tactics", presented at 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, 2002.

[28] B. Chess and G. McGraw, "Static Analysis for Security", IEEE Security & Privacy, Vol. 2, pp. 76-79, 2004.

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

[30] J. Viega and G. McGraw, Building Secure Software : How to Avoid Security Problems the Right Way : Addison-Wesley, 2001.

[31] B. W. Lampson, "Computer Security in the Real World", Computer, Vol. 37, pp. 37-46, 2004.

[32] D. Dasgupta, "Immuno-Inspired Autonomic System for Cyber Defense", Univ. of Mem-

phis, May 2004.
[33] L. F. Cranor and S. Garfinkel, "Secure or Usable?", IEEE Security & Privacy, Vol. 2, pp. 16-18, 2004.
[34] R. B. Vaughn-Jr., R. Henning, and A. Siraj, "Information Assurance Measures and Metrics : State of Practice and Proposed Taxonomy", presented at 36th Hawaii Int'l Conf. on System Science, 2003.
[35] S. Liu, J. Sullivan, and J. Ormaner, "A Practical Approach to Enterprise IT Security", IEEE IT Professional, Vol. 3, pp. 35-42, 2001.
[36] B. Martin, "Social Defense Strategy : The Role of Technology", Journal of Peace Research, Vol. 36, pp. 535-552, 1999.
[37] D. W. Straub and R. J. Welke, "Coping with Systems Risk : Security Planning Models for Management Decision Making", MIS Quarterly, Vol. 22, pp. 441-469, 1998.
[38] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks : Challenges and Solutions", IEEE Wireless Communications, Vol. 11, pp. 38-47, 2004.
[39] D. Armstrong, S. Carter, G. Frazier, and T. Frazier, "Autonomic Defense : Thwarting Automated Attacks via Real-Time Feedback Control", Complexity, Vol. 9, pp. 41-48, 2004.
[40] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Vol. 34, pp. 39-53, 2004.
[41] D. B. Parker, Computer security management. Reston, VA : Reston Publishing, 1981.
[42] K. A. Forcht, Computer security management. Danvers, MA : Boyd and Fraser, 1994.
[43] C. L. Smith, "Understanding Concepts in the Defense in Depth Strategy", presented at IEEE 37th Int'l Carnahan Conf. on Security Technology, 2003.
[44] D. J. Welch, N. Buchheit, and A. Ruocco, "Strike Back : Offensive Actions in Information Warfare", presented at 1999 Workshop on New Security Paradigms, Caledon Hills, Ontario, Canada, 1999.
[45] B. McKenny, "Defense in Depth", The Edge, Vol. 5, 2001.
[46] C. May, M. Baker, D. Gabbard, T. Good, G. Grimes, M. Holmgren, R. Nolan, R. Nowak, and S. Pennline, "Advanced Information Assurance Handbook", CERT/CC Training and Education Center CMU/SEI-2004-HB-001, Mar 2004.
[47] T. Grant and B. Kooter, "Comparing OODA & Other Models as Operational View C2 Architecture", presented at 10th Int'l Command and Control Research and Technology Symposium : The Future of C2, 2005.
[48] R. Bearavolu, K. Lakkaraju, W. Yurcik, and H. Raje, "A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks", presented at Military Communications Conference(MILCOM), 2003.

박 상 서

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