韓國 컴퓨터情報學會 論文誌
第8卷 第3號, 2003. 9.

2003-8-3-3-8

정보보안 침해 위험신호의 조직학습 실패에 관한 시스템 다이나믹스적 연구

박 성 진*

A Study on Risk Signal of Information Security and Organizational Learning Failure

Park, Sung Jin*

요 약

이 논문에서는 정보보안 분야의 각종의 위험신호(risk signal)에 대해 조직이 왜 적절한 대응을 하지 못하는 가를 조직의 구조적 측면에서 그 원인을 분석하고자 하였다. 위기는 갑자기 오지 않으며, 많은 경우 위기는 위기와 관련한 위험신호(risk signal)를 제기하면서 진전된다. 이러한 위험신호에 대해 적절하게 대응하는 경우, 위험은 새로운 기회를 만들어내게 되지만 그러하지 않은 경우 위험은 경제적, 비경제적인 측면에서 재난적인 결과를 초래할 가능성을 갖는다.

이 논문에서는 인과지도(causal diagram)을 이용하여 시스템적인 관점에서 환류하는 인과 고리의 관점에서 현상을 분석하는 시스템 다이나믹스적인 분석을 시도하였다. 분석결과, 조직의 성장과 업적 위주의 분위기가 일종의 압력이 되어, 안전에 대한 불감을 강화하게 되며, 이는 각종의 위험신호들에 내재된 위험성에 대해 과소평가하는 압력으로 작용하게 되는 점을 분석하였다. 이는 나아가서 기술적 기반에 대해 적절한 투자가 이루어지 못하게 하고, 정보보안과 관련한 학습을 적절하게 하지 못하도록 한 것으로 나타난다. 이 논문은 탐색적으로 정보보안 분야에서의 위험신호와 조직학습과의 관계를 분석한 탐색적 연구로서의 성격을 가진다.

* 경인여자대학 컴퓨터정보기술학부 부교수
※ 본 연구는 경인여자대학 교내연구지원 연구비에 의해 수행되었음.

Abstract

This study investigate the reasons of organizational failure in detection and appropriate response to risk signal. The Crisis does not come true suddenly, there is some risk signals in crisis. If Organization detect the risk signals the crisis is come true opportunities, if not the crisis is come true disastrous outcome.

This is use the system dynamics approach. System Dynamics assume the system as a collection of causal feedback loop, so we understand the dynamics around the problems. This investigate suggest that, the focus on growth is the a kind of promotional pressure and the pressure drive the organization to less attention the risk signal, so the risk is underestimate In proportion to real risk. Ultimate, the organization entrap the promotional climate and insensible to security. This study is a kind of hypothesis-discovering research, in the further study, the discovered hypothesis will be empirically tested.

▸ Keywords : Information Security, Risk, Learning Failure

Ⅰ. 서 론

오늘날 인터넷과 컴퓨터로 대표되는 정보통신기술의 발달은 사회변화의 새로운 동력으로 작용하고 있다. 이러한 정보통신기술의 활용은 경제적, 산업적 측면에서는 물론 사회 모든 부문에서 편의성의 증진, 생산성의 향상 등 많은 순기능적 효과를 만들어내고 있다. 그러나 한편으로는 정보통신기술은 새로운 위기를 초래할 수 있는 위험의 가능성을 제공하고 있다. 해킹, 컴퓨터바이러스, 프라이버시 침해, 음란, 폭력 정보의 범란, 사이버 공간에서의 인권침해, 사이버 범죄 등의 고의적 위험은 물론, 인적실수, 자연적 재해 등 각종의 새로운 위험에 노출되면서 이들 위험에 대한 적절한 대응의 필요성이 강조되고 있다.

정보보안 측면에서의 각종 위험은 이들이 실현되었을 때 경제적 손실을 비롯하여 바람직하지 않은 결과와 나아가서 재난적결과를 초래할 가능성을 가지게 된다. 이러한 점에 주목하여 기업은 물론 관공서등의 각종 조직체에서는 기술적, 정책적 차원에서 정보보안과 위험관리 측면에서 많은 노력을 기울이고 있다.

위험관리 정책적인 면에서 보면, 실제로 위험이 실현된 위기상황은 대부분의 경우 갑자기 오지 않는 것으로 나타난다. 위기는 위기의 진전과 관련한 각종의 징후, 조짐, 예보를 통하여 위험신호(risk signal)를 전제로 하여 전개되는 것으로 나타난다.

조직의 입장에서는 이러한 위험의 각종 징후들을 적절히 탐색하고 이에 필요한 준비예방과 대응을 하는 경우, 위험은 하나의 기회로 전환될 수 있지만, 그렇지 못한 경우, 위험은 크고 작은 경제적 손실은 물론, 재난적결과를 초래할 수도 있게 된다.

이 연구에서는 날로 증가하는 정보보안 침해 위협에 직면하여 각종의 정보보안 위험신호에의 적절한 탐색과 대응은 조직을 정보보안 침해 위험으로부터 안전하게 막을 수 있다는 가정 하에, 조직은 제기되는 위험신호에 왜 적절하게 대응하지 못하는지를 조직 학습적 관점에서 분석하고자 한다.

Ⅱ. 우리나라의 정보보안 침해 현황

인터넷 이용인구가 2002년 6월 기준으로 2,565만 명으로서 전체인구의 약 58%에 이를 정도로 정보화가 급격히 성숙되고 있다. 이에 따라, 기업은 물론 관공서등 전 분야에 걸쳐 정보시스템에 대한 의존도가 높아지고 있으며, 이는 효과적인 측면 이외에 한편으로 해킹이나 컴퓨터 바이러스 등 각종 정보화로 인한 폐해도 급격하게 증가하고 있는 것으로 나타난다. 2001년 한 해 동안 한국정보보호진흥원에 접수된 해킹 사고건수는 5,333건으로서 2000년 해킹사고 1,943건에 비해 274%나 증가한 것으로 나타나며, 2001년 2월부터 12월까지 한국정보보호진흥원과 주요 백신업체에서 접수받은 바이러스 신고건수는 65,033건에 이르고 있다 (정현철, 2002).

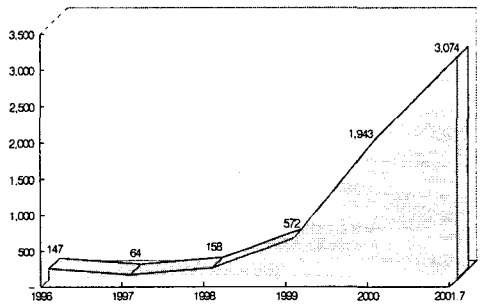

그림 1. 국내 년도별 해킹 사고 현황

인터넷의 전 세계적 보급이 가속화되고 정보화가 진전되면서 해킹 및 바이러스로 인한 정보보안 침해사고도 크게 증가하여 왔으며, 앞으로도 계속 증가할 것으로 나타난다 (정현철, 2002 ; 박정현, 2001).

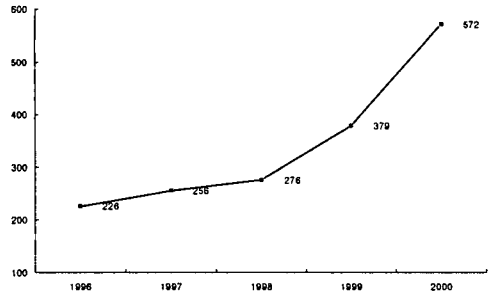

그림 2. 신종 컴퓨터 바이러스 발견 건수

정부 등의 공공기관도 예외는 아니어서 보안 침해사고의 급격한 증가 추세를 보이고 있다(국정원, 2001 ; 신영진, 2001). 국가정보원(정보보안119)의 자료에 의하면, 국가 및 공공기관에서 발생한 해킹사고는, 1998년도, 8건에서 2000년에는 102건, 2001년에는 507건으로 급격하게 증가하는 추세를 보이고 있다.

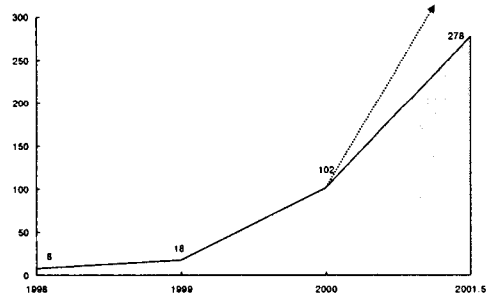

그림 3. 국가 및 공공기관의 연도별 보안침해

III. 위험신호와 위험의 수용

1. 위험과 위험신호

위험은 사람들에게 손실을 끼칠 가능성이 있는 일, 또는 바람직하지 않는 일이 일어날 가능성을 말한다. 그러므로 손실을 끼치거나 바람직하지 않은 일 자체가 위험이라기보다는 그러한 가능성이 있는 상태를 위험이라고 정의할 수 있으며, 이러한 위험이 실현된 상태를 위기라고 할 수 있다.

위기는 본질상 복잡하고 잘 정의되어져 있지 않으며 상호 연결되어져 있고 무질서하여 위기의 진전을 순차적으로 이해하기는 쉽지 않다. 그러나 많은 경우 위기는 갑자기 오지 않는다. 위기 위험신호(risk signal) 발생단계를 거쳐 위기의 실현단계로 진전되는 것으로 많은 연구들에서 나타난다.

일반적으로 위험신호는 포아송 분포적인 모습을 띠면서 발생하는 것으로 나타난다. 포아송 분포는 사건 발생 사이의 간격이 임의적임을 특성으로 하는데, 위험신호의 제기와 위기실현의 전체적인 모습은 대체로 포아송 분포를 따르는 것으로 나타난다. 포아송 분포에 의하면 위험신호의 발생사이의 간격은 위기실현에 이르기까지 점차로 짧아지는 경향을 가진 것으로 나타난다.

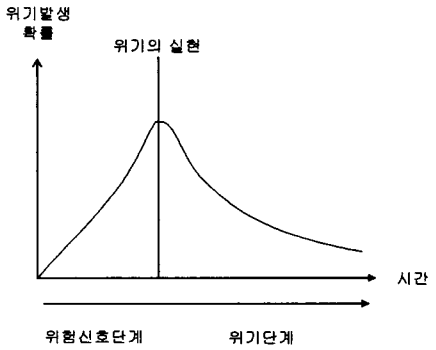

그림 4. 위험신호와 위기의 전개

2. 위험의 수용

2.1 위험수용의 주관성

바람직하지 않은 결과를 초래할 수 있는 가능성이 있는 위험이 실재로 실현되기 전에 그 가능성을 감지하고 숙지하여 적절하게 대응하는 경우 위험은 새로운 기회를 제공하게 되지만 그러하지 않은 경우, 위험은 재난적결과를 초래할 가능성을 내포하게 된다.

그러나, 일반적으로 제기되는 위험은 그 자체로서 사람들에게 수용되어 지기 보다는 일련의 위험에 대한 평가과정을 통해 수용되는 경향을 가진다. 즉, 위험은 주관적 인식과정을 통해서 그 위험성이 평가되는 속성을 가지고 있다는 의미가 된다.

이러한 관점에서 보면, 위험은 실제위험(real risk), 인식된 위험(perceived risk), 그리고 수용된 위험(acceptable risk)로 크게 구분된다.

(Blylock, 1985 ; Dake, 1992; Vlek and Saleen, 1981 ; Wildavsky and Dake, 1990). 즉, 실제 위험은 위험 인식주체와 관계없이, 어떤 행동이나 상황으로부터 나타난 실질적인 위험상황을 말한다. 인식된 위험은 개인적 경험과 인식과정, 그리고 조직적 특성화 환경에 의해 제약되어진 인식 주체에 의해 인식되어지는 속성을 말한다. (Korbin, 1982), 결국, 위험은 실재하는 위험과는 관계없이 사람들과 조직에 의해 각기 다르게 이해되어지는 속성을 가진다는 의미이다. 같은 위험도 개인과 집단, 조직의 구조와 특성에 따라 달리 경험되어지고 이해되어 지게 되며, 그 결과 각기 다른 위험에 대한 평가와 대응으로 이어질 수 있다는 의미가 된다. 수용된 위험(acceptable risk)은 자신의 목적이나 기준에 따라 참아낼 만한 정도로 인식하는 위험을 말한다. 즉, 수용된 위험은 위험에 대한 수용의 한계 값(threshold)에 해당하는 것으로 인식된 위험에 대한 대응을 결정하는 받아들일 말한 위험수준의 여부를 결정하게 된다.

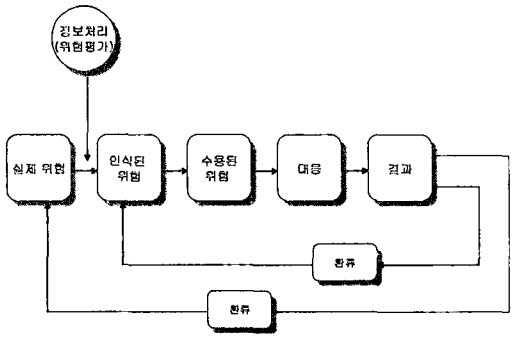

그림 5 위험의 수용과 대응

2.2 위험 수용 경향

위험수용은 개인적인 수용성향과 구조적인 수용경향으로 구분할 수 있다.

첫째, 심사숙고적인 위험수용(reasoned risk taking)이다. 이는 합리적인 비용이익에 근거하여 관련된 정보들에 대해 정확한 계산에 근거하여 다른 대안들이 더 나쁘기 때문에 위험을 수용하는 것이 가치가 있는 것으로 판단하거나, 실재 위험을 판단하는데, 개인적인 오류가 게재하여 잘못 판단하여 위험을 수용하게 되는 경우를 말한다.

둘째, 성향적 위험수용(dispositional risk taking)으로 이는 개인적인 신념이나 가치관에 의해 위험을 수용하는 경향을 말한다. 이러한 성향적 경향을 가진 개인이나 조직은 상황에 관계없이 일관되게 위험을 수용하거나 위험을 회피하게 된다.

셋째, 구조적 관계적 위험수용 경향(socially risk taking)이다. 이는 개인적인 합리적인 인지과정이나 개인적인 속성에 의한 것이기 보다는 다른 사람과 조직등과의 관계적 속성에 의해 틀 지워는 위험수용 경향을 말한다. 위험을 수용하게 하는 사회적 영향력으로는 동료들의 압력, 앞선 행동에 대한 몰입 등의 현상으로 나타난다.

2.3 위험의 수용과 조직학습

조직 학습은 오류에 대한 교정능력차원과 환경적응 차원에서 이해되어 진다. 학습조직이란 "개인의 학습능력이 조직 전체로 확산 공유되어 제도화, 체계화되어 환경에 대한 적응력이 높은 조직"으로 정의할 수 있다.

학습조직의 개념에 의하면 위험신호에 대한 대응은 문제를 발견하고 교정하며 기존의 결정규칙이나 가치 체계 내에서 해결이 불가능한 경우, 근본적으로 조직의 구조적, 내재적 변화를 도모하여 적극적으로 문제 해결을 시도하는 경우를 말한다.

3. 위기관리

3.1. 위기의 개념정의

위기에 관한 개념은 제대로 정의되지 않고 남용되는 경향이 있다(Pauchant & Mitrofff, 1992, 11).

위기(crisis)는 사고(accident), 갈등(conflict), 기술적 실패(technical failure), 사소한 상황(trivial circumstances) 등과 함께 혼재되어 사용되는 것으로 나타난다.

개념상의 혼돈을 피하기 위하여 Hermann(1963)의 고전적 정의에 의하면 위기는 "사람을 놀라게 하고 대응을 강구할 시간을 제약하고 상위 수준의 목적달성을 위협을 가하는 사건"으로 정의한다. 이러한 고전적 정의를 바탕으로 개념의 정립에 관한 많은 연구들이 있어왔다.

위기의 일반이론을 제시하고자 한 Perrow(1984)는 위기를 관련된 구성요소들 간의 상호작용의 측면과 연계의 측면에서 위기를 분류하였다.

Perrow는 복합적 상호작용을 예측이 어려운 순서로 발생하며 계획하거나 예측하지 못한 순서에 따라서 비가시적으로 혹은 즉각적인 파악이 어려운 상태에서 이루어지는 상호작용을 말한다. 단선적 상호작용은 예측된 순서에 의하여 발생하며 계획하지 않았더라도 가시적으로 상호작용이 이루어지는 경우를 말하고 있다. 한편 긴밀한 연계와 느슨한 연계차원은 구성요소들 간의 반응적 결합관계를 나눈 것으로

구성요소들 간의 고유한 특성이 유지되며 물리적으로 분리되어지는 경우를 말하고 있다.

연계성 \ 상호작용	단선적	복합적
긴밀한 관계	시스템 실패적 위기 (가공할 만한 알려진 위기)	포스터모던 위기 (가공할 만한 미지의 위기)
느슨한 관계	하위 시스템적 위기 (국지적, 예측 가능한 위기)	일상화된 위기 (국지적, 예측 불가능한 위기)

표 4. 위기의 유형

Perrow에 의하면 각종의 정보보안 사고는 일종의 관련된 상호작용을 예측가능하지 못하며, 관련된 구성요소들이 네트워크를 통해 긴밀하게 연계되어 일단 문제가 발생하면 그 손실이 가공할 만한 정도의 포스터모던 한 위기의 일종으로 분류할 수 있다.

3.2 위기를 이해하는 시각

위기를 이해하는 일반적 시각은 다양하게 구분할 수 있다. 이들 시각을 구분하면 다음의 세 가지로 구분할 수 있다.

첫째, 위기는 사람이나 조직이 사용하는 현대적 기술 그 자체에 내재하는 복잡성(complexity)에 의해 우기가 발생한다는 시각이다. 이는 사소한 일상적 오류나 문제가 누적되면서 재난적 결과를 초래하게 된다는 입장이다. 이의 대표적인 학자는 C.Perrow를 들 수 있다. 이러한 입장에 서면, 컴퓨터와 인터넷으로 대표되는 정보통신 기술의 발달과 이의 활용은 불가피 위험을 내포하게 되며, 이로 인하여 어느 정도의 기술적 실패와 이로 인한 위기는 감수할 수밖에 없게 된다.

둘째, 위기는 사람이나 조직의 잘못된 판단에 의해 야기될 수 있다는 입장이다. 이는 기술적으로 결함이 없다고 하더라도 인간의 악의적인 의도나 실수, 잘못된 판단 등으로 인하여 위기가 초래될 수 있다는 입장이다.

셋째, 위기는 기술적 결함과 인간의 오류적 속성에 의해 촉발되는 종합적인 입장에서 이해한다. 어느 한 요인에 의해 문제가 발생하면 이는 복잡한 체계 내에서 확대 재생산되면서 사소한 원인이 큰 재난적 결과를 초래하게 된다는 입장이다.

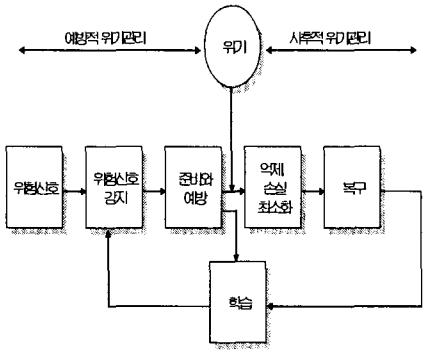

그림 6. 위험신호와 위기관리

Ⅳ. 정보보안에서의 위험

1. 정보보안 위험의 원천

정보보안에서의 위험은 논의하는 사람마다 다양하게 정의되어 질수 있다. 고의성에 따라 사람의 실수로 인한 위험, 의도적 위험으로 구분할 수 있으며, 위험의 원인과 출처에 따라 악의적, 비의도적, 물리적 위험으로 구분되기도 한다.

ISO 7482-2에 의하면 정보보안 분야의 위험은 불법적 제휴(illegal associations), 비인가 된 접근(non-authorized access), 정보의 누출(leakage of information), 정보 전송량의 분석(traffic analysis), 데이터의 수정 또는 파괴(data modification or destruction), 메시지 순서변경(invalid message sequencing), 부인(repudiation), 서비스 방해(DoS; Denial of Service)등이다.

정보보안의 위협 원천에 따라 정보보안의 위험요소를 분류하면 화재, 수해, 지진, 정전 등의 자연재해로 인한 위험, 사람에 의한 의도적 위험요인, 사람에 의한 비의도적 위험, 정보시스템의 결함 등으로 구분할 수 있다. 사람에 의한 의되적 위험은 하드웨어에 대한 물리적 공격, 절도 등의 물리적 공격과, 시스템 자원의 불법사용, 불법적 접근, 사용 방해, 위조, 위장, 유해 프로그램의 삽입, 망분석 등 기술적 공격 등으로 구분할 수 있다. 사람에 의한 비의도적 위험은 조작미숙, 실수 등에 의한 위험을 말하며, 정보시스템의 결함은 운영체제의 결함, 프로그램의 결함, 과부하, 하드웨어 고장 등을 말한다.

2. 정보보안 침해 공격유형

정보보안에서의 위험은 적극적인 공격에 의해 발생할 가능성을 가진다. 정보보안에 대한 공격의 종류는 방해(Interruption),가로채기(Interception),불법수정(Modification),위조(Fabrication)등으로 구분된다.

또한 이들 정보보안에 대한 공격은 구체적으로 해킹(hacking),컴퓨터 바이러스(malicious code), 컴퓨터 조작 오류 및 삭제(omissions),내부자 사보타지(employee sabotage), 사이버 테러 등의 형태로 나타나고 있다.

컴퓨터보안연구소(Computer Security Institute)와 샌프란시스코 미 연방 수사국 컴퓨터범죄수사단(San Francisco Federal Bureau of Investigation's Computer Intrusion Squad)이 함께 조사한 2001년도 컴퓨터 범죄 및 보안에 대한 설문조사 결과에 의하면, 정보보안 분야에서 공격은 첫째, 조직들이 내외부로부터 사이버 공격을 받고 d있다. 둘째, 광범위한 사이버공격이 탐지된다. 셋째, 사이버공격은 심각한 경제손실을 초래할 수 있는 특성을 가진다(황성원, 2001).

V. 정보보안 위험신호에 대한 조직학습 실패의 원인분석

1. 분석방법

이 논문에서는 위험과 위험에 대한 대응을 이끌어내는 위험의 평가과정을 중심으로 위험신호에 대한 조직학습 실패의 원인을 분석하고자 한다.

분석에 사용된 기법은 시스템 다이나믹스의 인과지도(causal diagram)분석 방법이다. 시스템 다이나믹스는 조직, 사회를 포함한 모든 시스템의 역동적인 변화 매커니즘을 비선형적인 피드백시스템으로 파악하고 시스템의 행태에 주로 관심을 두고 분석하는 연구방법이다. 시스템 다이나믹스는 Forrester(1961)에 의해 체계화된 이후, 다양한 분야에서 동태적인 연구방법론으로 확산되어 왔다.

시스템 다이나믹스는 1980년대 들면서 시스템 사고(system thinking)라는 용어로 통용되기 시작하였으며, Peter Senge에 의해 보편화되기 시작하였다.

시스템 다이나믹스의 기본도구는 피드백 고리를 바탕으로 하여 강화 고리(중요 변수가 기하급수적인 상승이나 강하를 하는 경우) 균형 고리(시간지연 없이 목표를 향해 움직이거나 시간지연에 따라 목표 선상을 넘나드는 경우), 시간지연(delay)라는 세 가지 핵심개념들로 구성되어 있다. 시스템 다이나믹스의 고유한 방법론적 특성은 시스템의 동태적인 행태변화, 즉 시간의 경과에 따른 시스템의 행태변화에 관심을 둔다는 점과 이러한 동태적인 변화의 근본적인 원인을 피드백구조에서 찾는다는 점이다.

방법론상으로는 시스템 다이나믹스는 시스템 모델링과 컴퓨터시뮬레이션 그리고 인과지도 분석방법으로 구분되어 적용된다. (김동환, 2002). 시스템의 동태적인 행태를 분석하고자 할 때는 주로 시스템 다이나믹스 모델링과 컴퓨터 시뮬레이션 방법이 적용되고, 정태적인 시스템의 구조를 분석하고자 할때는 주로 인과지도 분석방법이 활용되고 있다(김동환, 1997).

이 연구에서는 위험 신호에 대한 적절한 대응을 하지 못하는 복잡하게 연결된 정태적 구조에 관심을 가진 것으로 인과지도 분석 방법을 주로 이용하고자 한다.

2. 위험의 평가와 위기관리

정보보안은 기본적으로 자기강화적(self-reinforcing)환류과정을 거친다고 볼 수 있다. 즉, 위험에 대한 지각과 위험에 대한 주의를 더욱더 기울이는 한 위험에 대한 대응을 충분히 함으로써 재난적 결과를 줄일 수 있게 된다. 이는 아래 그림에서 R1(위기관리 고리)로 설명될 수 있다. 즉 위험신호가 제기되면 이에 대해 충분히 주위를 기울임으로써 위험에 대한 평가를 제대로 하게 되고, 그 결과 적절한 사전적 대응과 예방노력을 통해 결과를 줄일 수 있게 된다.

대응결과로부터 다소간의 시간지연과 장애가 존재하기는 하지만, 이러한 결과로부터 학습을 하게 됨으로써 추가적인 위험신호에 대한 감지와 대응을 더욱더 잘 할 수 있게 되는 고리를 말한다. 대응 결과는 보안 인프라의 강화, 보안의식의 고취등 관련한 조치가 취해짐으로써 위험에 대한 학습과 이로 인한 위험 신호에 대한 적절한 대응체계를 갖추게 되는 구조를 가지게 된다는 것이다.

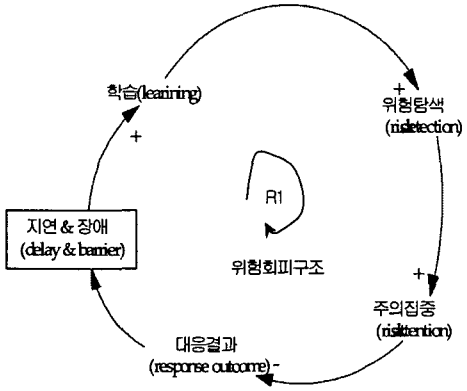

그림 7. 위험 회피 강화 구조

3. 위험 과소평가의 촉진과 안전 불감의 강화

그러나 조직의 입장에서는 한정된 자원을 통해 조직의 목표를 달성하고자 하는 유인을 갖게 된다. 이러한 조직의 관점에서 보면 정보보안적인 측면은 직접적인 성과를 나타내는 측면이라기보다는 만약 위험이 실현되었을 때 재난적 결과를 가져오는 속성을 갖고 있다.

즉, 조직의 입장에서는 목표 달성과 관련된 노력과 이에 대한 기여를 통해, 구성원들의 성과를 높이고 이를 통해 더 많은 업적과 보상을 받고자 하는 유인을 갖게 된다.

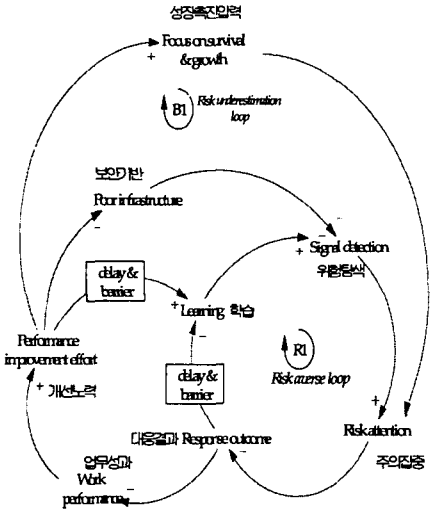

그림 8. 위험의 과소평가 강화고리

이는 '안전에 대한 불감' 문화를 촉진하게 되며 더욱더 위험신호에 대해 둔감하게 대응하고 더욱더 위험에 대해 과소평가하게 하는 작용을 할 가능성을 갖는다.

조직의 입장에서는 성장적인 측면에 더욱더 강조가 주어지는 경우, 안전 불감문화는 더욱더 약화되게 되고, 성장에 대한 기여와 이를 통한 더 나은 업적을 만들어내기 위한 '성장 촉진적 문화'가 강조될 가능성을 갖는다.

이러한 조직 구조 하에서는 성장적인 면에 대한 노력과 주의집중(attention)이 더욱더 강화 되어 위험에 대해 불감하게 된다.

VI. 결론 : 성장촉진압력과 안전 불감 문화의 확산

이상에서는 날로 증가하는 정보보안 사고에 주목하여 정보보안의 위험성을 경고하는 각종의 위험신호(risk signal)에 대해 왜 기업이나 정부가 적절하게 대응하지 못하는 가를 구조적인 관점에서 분석하였다. 위험의 실현은 재난적결과를 초래할 가능성을 가지며, 이러한 위험에 대한 적절한 인식과 안전문화의 확산, 위험대응 체계의 마련은 정보화의 진전과 함께 대단히 중요한 문제로 등장하고 있다.

분석결과, 조직의 경우, 성장과 목표달성이라는 촉진압력이 강조되면 강조될수록 상대적으로 위험문제와 같이 실현되면 재난적결과를 가져오지만 실현의 가능성이 적은 위험의 문제에 대해서는 상대적으로 과소평가하는 경향을 가지게 되며, 이로 인해 안전에 대한 불감문화가 확산될 수밖에 없는 구조적 특성을 갖게 되는 것으로 나타났다. 이러한 구조적 환경 하에서는 정보화의 진전과 함께 발생 가능한 해킹, 바이러스 등 각종의 정보보안 침해 위험과 관련하여 제기되는 각종의 위험신호에 대해서도 적절한 주의집중(attention)과 적절한 사전적 사후적 대응을 통하여 위험을 최소화하기 어렵게 되는 구조를 살펴보았다.

이 논문에서는 관련된 주제에 대해 탐색적 목적으로 인과지도 분석방법을 통해 위험에 대한 대응 구조를 분석하였다. 향후에 실증적인 자료를 통하여 조직의 촉진압력의 강화와 안전 불감 문화의 확산, 이를 통한 위험에의 노출과 학습실패에 대해서 실증적으로도 분석하고자 한다.

참고문헌

[1] 안문석, 박성진, 맹보학, 2003, 전자정부 정보보호 대응체계 구축 방향에 관한 연구, 한국정보보호학회, 2003

[2] 김도훈, 문태훈, 김동환, 시스템다이나믹스, 1999, 대영문화사

[3] 김동환, 인과지도 시뮬레이션 방법론, 한국시스템 다이나믹스 연구, 2002

[4] 한국인터넷정보센터, 한국인터넷통계집, 2002.

[5] 정현철, "2001년 해킹·바이러스 사고를 돌아보며", 정보보호뉴스, 통권54호, 2002.

[6] 박정현, "국내 해킹사고 분석 및 대응기술", 제6회 정보보호 심포지엄, 2001.

[7] 정보보호산업협회, 국내·외 해킹 등 사이버테러 사례분석 및 피해규모 분석에 관한 연구, 한국정보보호센터, 2000.

[8] 국가정보원, "2000년도 국가·공공기관 해킹사고 5.7배 급증", http://www.nis.go.kr/119, 2001.

[9] 신영진, "국가·공공기관 해킹사고 현황 및 지원", 제6회 정보보호 심포지엄, 2001.

[10] 국가정보원, "2001년도 국가·공공기관 해킹사고 현황 및 통계". http://www.nis.go.kr/119, 2002.

[11] Fishjoff, Barruch, Sarah Lichtenstein, Paul Slovic, Stephen L. Derby and Ralph L. Keeney, Acceptable Risk, Cambrage Univ, 1981

[12] Kaufman, Herbert, Adminstrative Feedback, Washington D.C., 1973

[13] Pauchant, Thierry, Ian I. Mitroff, Transforming The Crisis Prone Organization, Jossey-Bass Publisher, 1992

[14] Perrow, Charles, Complex Organizations, New York, 1986

[15] Senge, Peter, The Fifth Displine, A Currency Book, 1990

[16] Vertzberger Yaacov, Risk Taking and Decisingmaking, Stanford Univ., 1998

저 자 소 개

박 성 진

1999 고려대학교 박사 (전공 : 정보체계)

현재 경인여자대학 컴퓨터정보기술학부 인터넷비즈니스전공 부교수

〈관심분야〉 정보체계, 전자정부, 정보정책