조직의 적정 정보 보안 수준 결정을 위한 목표 잉여 위험의 결정 방법

*김정덕· **이성일

Determination Method of Target Residual Risk for Proper Information Security Level Determination

*Kim-jungduk, **Lee-sungil

요약

현재의 조직 환경에서 정보 보호 수준의 결정은 필수 불가결한 이슈가 되고 있지만 정보 보호 수준 구축을 위한 기준은 상대적으로 부족한 실정이다. 이에 본 논문에서는 정보 보호 수준 결정에 있어서 기준이 될 수 있는 중요한 요소인 위험에 대해서 기존의 위험 평가 프로세스를 분석하여 개선된 위험 평가 프로세스를 제시하고 허용 가능한 위험을 결정하기 위한 중요 기준인 목표 잉여 위험의 결정 방법에 대해 논하고자 한다.

Key words: TRR(Target Residual Risk), RAC(Risk Accept Criteria), TPL(Target Probability Level), TLL(Target Loss Level)

1. 서론

시스템이나 네트워크 혹은 기타 모든 응용시스템 보안을 위한 프레임워크 설계 시 위협 및 위험 평가 프로세스 구축은 필수적인 절차이다. 그러나 발생할 수 있는 모든 위험을 고려하고 그에 대한 완벽한 대비책을 구축하는 것은 불가능하기도 하겠지만 이에 따른 막대한 비용이나 시간 문제 때문에 100 % 위험이 제거된 시스템 구축도 불필요할 수 있다. 따라서 특정 조직에서의 허용 가능한 위험(Acceptable Risk)을 결정하고 이를 위한 올바른 대안을 설정하는 것은 보안 관리에서 매우 중요한 프로세스 중에 하나이다. 허용 가능한 위험을 결정하기 위한 중요한 기준이 목표 잉여 위험(Target Residual Risk, 이하: TRR)인 것이다.

1980년대 중반부터 선진국들의 보안 정책 변화로 인해 보안 대책 결정 시 위협 및 위험 평가 프로세스 이용을 요구하게 되었다. 하지만 기존의 위협 및 위험 평가 프로세스는 허용 가능한 위험과 그러한 위험의 위험수준 결정을 위한 정확한 방법론을 제시하지 못하였다. 기존 위협 및 위험 평가 프로세

* 중앙대학교 정보시스템학과 부교수
** 중앙대학교 정보시스템학과 석사 4 차

스는 "Ready, Fire, Aim"의 구조를 나타내고 있는데 이러한 구조는 보안 실무자가 위험을 분석하고 권고 사항을 설정한 후에 상부 관리층이 허용 가능한 위험을 결정하는 구조적 모순을 내재하고 있는 것이다. 즉, 허용 가능한 위험은 조직 전체에 걸쳐 위험을 평가하고 대비책을 구축하는데 있어 지침과 같은 성격을 띄고 있으므로 위험 분석 프로세스 구축 전에 이미 결정되어 있어야 하지만 현재의 구조는 프로세스가 구축된 후에 프로세스의 목표를 설정하는 양상을 나타내고 있는 것이다. 특히 현재의 위협 및 위험 평가 방법론은 허용 위험이 위협 및 위험 평가 프로세스 구축 시 근간이 되는 정보임에도 불구하고 그에 관련된 의사 결정을 위한 특정한 절차를 제시하지 못하고 있다.

따라서 본 논문에서는 다음과 같은 4 가지 의문 사항에 초점을 맞추어 해결책을 모색하고자 한다.

1) 위협 및 위험 평가 프로세스의 어느 단계에서 TRR이 결정되는가?
2) 누가 TRR을 결정하는가?
3) TRR을 결정할 때 고려해야 할 요인은 무엇인가?
4) TRR을 위한 정확한 위험 수준을 어떻게 결정하는가?

첫 번째 의문 사항을 해결하기 위해서는 현존 위협 및 위험 평가 프로세스에 대한 분석에 기초하여 보다 실효성 있게 개선된 프로세스를 제시하고, 단계 별로 업무 내역을 살펴봄으로써 TRR이 결정되어야 하는 단계를 결정하고자 한다. 두 번째와 세 번째 의문 사항은 위험에 대한 의사결정 과정과 고려 사항 및 주체를 결정함으로써 해결할 수 있으며 네 번째 의문 사항은 위험 수준과 민감도 분석 과정을 통해 해결될 수 있다.

본 논문에서는 기존 위협 및 위험 평가 프로세스의 분석을 통해 기존 프로세스의 한계점을 도출하고 한계를 극복할 수 있는 새로운 위협 및 위험 평가 프로세스를 제시하고자 한다. 또한 제시된 프로세스에 따른 위험 수준 정의, 민감도 분석, 손해 수준 결정, 발생 확률 측정 방법을 소개하며 이를 토대로 목표 잉여 위험(TRR)과 위험 허용 기준(Risk Accept Criteria:이하 RAC)을 결정하고 사용 방법을 서술하고자 한다.

2. 기존 위험 평가 프로세스

2.1 위험 평가 패러다임의 변화

비용이나 이윤 분석에 기초한 위험평가는 보안을 위하여 제한된 자원을 활용할 수 있는 합리적인 방법을 제공해 준다. 이러한 위험분석은 계량화가 가능한 분야에서는 매우 유용한 패러다임이다.

상업적인 목적의 위험평가 접근법은 다각도로의 발전과 개선을 거듭하고 있다. 예를 들어 미국의 Atena 보험 회사는 정보시스템이 목표한 기능을 수행하지 못할 경우 회사가 도산할 수도 있다는 사실을 인지하고 정보시스템에서 발생 가능한 위험과 회사에서의 위험을 통합하여 관리하기 시작하였다. 하지만 이러한 통합적 위험 관리 역시 개선되어야 할 사항은 여전히 존재하고 세부적으로 프레임워크를 결정해야 하는 과제를 안고 있다. 따라서 학자들은 지속적인 위험평가 패러다임의 변화를 주장하고 있다.[Hilary H. Hosmer,1996]

제 1 세대 위험평가는 메인프레임 환경이고 모든 시스템에 적용가능하며 사전에 정의된 위험 수준에 준거하는 정도에 의존하는 등급 시스템(Rated system) 패러다임이다. [Hilary H. Hosmer,1996]

제 2 세대 위험평가는 자산 보호 패러다임으로써 위험평가 도구가 출현하였고 특정 시스템에 대한 위험 평가 필요성이 대두되었으며 시스템적 관점과 분석 도구가 사용되었다. 제 2 세대 위험 평가의 장점은 수동적, 능동적 위협을 고려하는 것이고 여러 수준의 보안 대책이 인식되고 있는 것이다. 반면 한계점은 보장에 대한 모호성으로 인한 위험감소 측정 문제와 보안 외에 안전, 신뢰성을 포함하는 통합적 관점이 결여되어 있다는 것이다.
[Hilary H. Hosmer,1996]

이제 위험 평가의 경향은 제 3 세대 위험평가로의 추세를 나타낸다. 제 3 세대 위험평가는 전반적인 위험 관리 패러다임으로써 시스템 유연성과 보안의 균형적 시각을 통한 정확한 시스템 운영에 초점을 두고 있으며 동적이고 전체 시스템에 걸친, 시스템 생명주기 전반에 걸친 위험관리이다.
[Hilary H. Hosmer,1996]

위험 평가는 정보시스템을 어떻게 보느냐에 따라 크게 달라진다. 전체 시스템을 수용하려는 시각보다는 비용과 요구에 기반하여 최적의 보안방법을 얻을 수 있어야 한다.
[Hilary H. Hosmer,1996]

2.2 기존 위험 평가 프로세스의 분석 및 한계점 도출

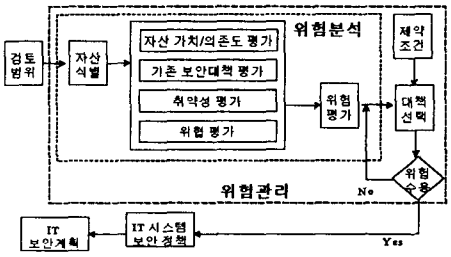
위험에는 손해(혹은 손상)와 발생 확률이라는 두 가지 일반적인 속성이 포함되어 있다. 손해는 보안대책에 의한 위험의 감소 및 예방에도 불구하고 위협 사건이 조직의 목표, 성취능력과 자산에 영향을 미치는 정도를 비용이나 한계치로 환산한 것이고 발생확률은 자산, 작업활동 같은 특정 작업 기간의 전주기에 걸쳐 사건이 발생할 수 있는 기회를 말한다. 현재 공공기관에서는 위험을 "취약점이 실제 발생할 수 있는 기회"로 정의하고 있다. 하지만 공공기관에서 정의한 단순한 정의는 여러 가지 문제점을 안고 있고 그러한 문제점을 정리해 보면 다음과 같다.

- 손해 정도를 간과한 채 단지 발생 확률에만 초점을 두고 있다.
- 위험을 표현하는 방식이 위험 평가 프로세스의 목적을 충분히 충족시키지 못한다.
- 위험의 개념이 너무 포괄적이어서 보안 대책으로 해결할 수 있는 범위를 벗어나므로 보안대책에 의해 완화되는 것이 불가능하고 보안대책 발효 후의 잉여 위험이 제외된다.

기존의 발생확률을 재검토하기 위해서 기존의 위험평가 프로세스 내에서 발생확률 결정에 관한 사항을 검토해 보아야 한다. 기존 위험 평가 프로세스에서의 발생확률 수준은 다음의 4 가지로 분류되어 있다.

- 고려가치 없음: 위협이 발생하더라도 검토 대상으로서 가치가 없다.
- 저(低): 위험 발생 사례는 전혀 없고 발생 가능성이 희박하다는 전제하에 위협이 고려될 수 있다.
- 중(中): 발생 사례가 거의 없지만 존재하고 발생 가능성은 충분하다는 전제하에 위협이 고려될 수 있다.
- 고(高) : 중요 발생 사례가 존재하여 검토된 경험이 있고 발생 가능성이 높다는 전제하에 위협이 평가된다.

기존의 위험 평가 프로세스의 발생확률 수준에 내재된 문제점은 수준의 분류가 너무 정성적이기 때문에 분류 자체는 용이하지만 수준 결정이 모호한 경우가 많이 발생할 수 있다. 그리고 과거의 데이터에 대한 지나친 의존성으로 인해 새로운 위협의 발생시 대처가 불가능하다. 또한 수준 설정 실무자의 지나친 주관성이 객관적인 수준 결정을 방해할 가능성이 크다. 위험을 서술하거나 측정하기 위해서는 두 가지 속성이 개별적으로 측정되어야만 한다. 기존의 세부적인 위험 평가 프로세스는 다음의 <그림 2-1>과 같다.



<그림 2-1> 기존 위험 평가 프로세스

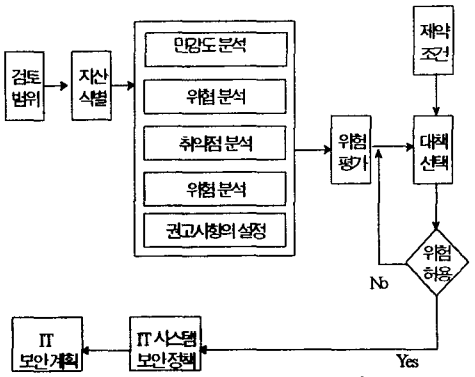
기존 프로세스에서의 한계점은 <그림 2-1>에서 나타난 바와 같이 위험 관리자가 위협과 위험을 분석하고 권고사항을 준비한 후 상부 관리층에서 허용 가능한 위험을 결정하는 분석과 결정 사이의 모순을 들 수 있다. 이러한 경우 위험관리자가 위협 발생을 보고하지 않았을 경우 상부 관리층이 위험을 처리하는 것이 불가능하게 될 수 밖에 없다. 그리고 잘못된 보호 대상을 결정하고 처리하였을 경우 자원의 낭비에 대한 책임 소재의 문제가 발생하게 된다. 이러한 문제점을 방지할 수 있는 대안은 사전에 TRR을 결정하여 위험관리자가 위험 분석 업무를 수행하기 전에 상부 관리층이 제시한 허용 가능한 위험 수준(TRR) 내에서 위험관리자에게 분석 방향을 설정해 주는 방법이 있을 수 있다.

기존 위험 분석 프로세스에서 개선이 필요한 사항은 보안 실무자와 관리층이 반드시 허용 가능한 위험 수준의 정도를 통일하여야 하고 이것은 위협 및 위험 평가 프로세스에서 위험 평가 수행 전에 이루어져야 한다. 관리층은 위협 및 위험평가 프로세스의 시작 단계에서 적어도 임시로 결정된 목표 잉여 위험(TRR) 정도는 문서화하여 위험관리자에게 제공하여야 한다. 제공되는 위험 허용치는 조직의 역할이나 목표에 관련된 방식으로 정의되어야 한다. 역할/목표, 핵심기능, 프로세스들, 그리고 업무 관련 자산/자원들은 민감도 분석 프로세스 내에서 취급되어야만 한다. 시스템을 사용하는 현업 관리층은 보안실무자와 시스템 엔지니어의 능력을 동원하여 민감도 분석을 수행하여야 한다. 이렇게 수행된 민감도 분석은 적절한 수준의 현업 관리층에 의해 서명· 승인되어야 한다. 초기의 TRR은 보안 실무자의 지원을 받을 수 있는 적절한 수준의 현업 관리층에 의해 개발되어야 한다. 이러한 개선 사항을 통해 개선 위험평가 프로세스 모델이 결정될 수 있다.

3. 위험 평가 프로세스의 개선

3.1 개선된 위험 평가 프로세스

이전 단락에서 개략적으로 제시한 개선사항을 기반으로 개선된 위험 평가 프로세스를 제시하면 다음의 <그림 2-2>와 같고 <그림 2-1>에서는 개별적인 프로세스로 나뉘어져 있던 검토 범위 결정, 자산 식별, 자산 가치/의존도 평가 프로세스들이 민감도 분석이라는 하나의 프로세스로 통합되고 위험 분석의 기반 정보로 이용되고 있다.



<그림 2-2> 개선된 위험 평가 프로세스

1 단계 : 민감도 분석

이 단계에서의 주요 목표는 민감도 분석을 통해 핵심 보호 대상을 결정하고 보호 대상 선정 근거를 확립하는 것이다. 그리고 관리층에서 적어도 임시로 결정된 TRR과 RAC를 제시하여야 한다. 민감도 분석은 보호 대상(자산)들의 민감도를 분석함으로써 그들의 보호 근거와 우선 순위를 식별하기 위해 실행되는 프로세스이다. 민감도 분석 시 주요 목표, 능력, 기능, 프로세스, 역할/목표를 성취하기 위해 필요한 작업과 그러한 작업을 수행하기 위해 필요한 자산/자원을 고려해야만 한다.

특정 자산의 중요성/가치를 파악하기 이전에 자산에 대해서 위험을 허용할 수 있는 정도를 결정하

는 것은 불가능하다. 민감도 분석을 통해 조직과 관련 업무 기능에 대한 자산의 전략적, 운영적, 전술적 민감도 및 가치를 파악할 수 있으므로 민감도 분석의 결과는 TRR을 결정하기 위한 중요한 자료가 된다. 원활한 민감도 평가 작업을 위해서는 현업 경영층의 지원이 필수적인 요소이다. 민감도 분석 프로세스는 다음의 5 단계를 거쳐서 결과물을 산출한다.

- 조직의 역할/목표 결정
- 보호 대상 결정
- 각각의 자산에 대한 민감도 결정
- 본질적인 보안 관심사 결정
- 민감도 분석 결과에 대한 승인

2 단계 : 위협 분석

주어진 자산/자원에 대한 위협을 분석하는 단계로서 주요 목표는 자산/자원을 손상시키는 위협을 식별하고 위협이 발생하는 조건을 분석하는 것이다. 이 단계에서의 분석 결과는 위협 평가로서 문서화되어야 한다.

3 단계 : 취약점 분석

자연 재해(예: 홍수, 지진)에 자산/자원이 노출되거나 인간의 고의적인 행위로 인해 자산/자원이 손해에 노출될 수 있는 상황/조건을 분석하는 단계이고 주요 목표는 다음과 같다.

- 자산이 자연 재해로 인해 노출되는 상황/조건 식별
- 자산이 공격에 노출되는 상황/조건 식별
- 자산이 자연 재해에 노출되는 방식 분석
- 자산 공격의 난이도 분석
- 위협을 가하는 공격자들이 자산을 공격하기 위해 상황/조건을 이용하는 방법 분석

이러한 취약점 분석의 결과는 취약점 평가로서 문서화되어야 한다.

4 단계 : 위험 분석

발생 가능한 자연재해와 계획적 공격으로 인한 예상 손해 값에 근거하여 손해 정도를 결정하기 위해서 처음 세 단계의 분석 결과를 조합하는 단계이다. 주요 목표는 자산에 손해를 입히는 사건을 분석하고 그러한 사건에 의한 피해정도를 분석하며 발생원인을 분석하고 손해의 허용 여부를 결정하는 것이다. 위험분석의 결과는 위험 평가로서 문서화된다.

5 단계 : 권고사항의 설정

권고사항은 허용 불가능한 위험을 취급하기 위한 대안을 관리층에게 제공하기 위해 보안 실무자에 의해 개발된다. 권고사항을 설정하는 목적은 적절한 보안 업무를 구축, 유지보수, 재설치하는데 있다. 권고사항에 포함될 수 있는 사항은 다음과 같다.

- 보안대책 구현/개선에 의한 위험 축소 방법
- 운영 방식 변경에 의한 위험 회피 방법
- 불필요한 예방책의 제거/축소
- 업무 지속성(Business Continuity) 혹은 여타 비상 계획의 사용에 의한 위험 취급 방법

권고사항은 보안 실무자에 의해 문서화되고 관리층에게 보고되어 승인을 받아야 한다. 관리층의 승인은 권고사항 구현을 위해 필요한 자원 이용 동의를 의미한다. 권고사항은 반드시 다음과 같은 의문사항에 대한 해답을 제시해야 한다.

- 허용 불가능한 위험을 축소/회피하거나 불필요한 안전대책을 축소/제거하기 위해 수행되어야 할 작업은 무엇인가?
- 그러한 행위의 우선순위는?
- 각각의 행위에 대해 시간당 비용, 자원 운영의 영향, 기회 비용은?
- 권고된 행위의 비용 효율성은?

3.2 위험수준의 개선

2 장에서 기술한 바 있는 공공기관 위험 정의의 문제점을 고려하여 새롭게 위험을 정의하면 다음과 같이 구체적으로 기술될 수 있다.

- 위험은 위협사고 발생에 원인이 되는 취약점 노출의 가능성과 위협 사고로 인해 자산에 미치는 손해의 정도
- 위험은 자산, 위협, 취약점들을 조합한 결과이다.
- 고유 위험: 안전대책이 구현되기 이전에 존재하는 위험, 자산· 위협· 고유 취약점의 조합 결과
- 잉여 위험: 안전대책이 구현된 후에 남겨진 위험, 자산· 위협· 잉여 취약점 조합의 결과 [D.A. Stolovitch and L.D. Robertson]

위험수준은 손해수준과 발생확률 수준을 조합하고 단일한 값으로 환산하여 하나의 레이블로 합쳐서 표현하는 방법이 있고 손해 수준과 발생확률 수준을 각각 독립적으로 계산하여 두 개의 레이블로 나누어 표현함으로서 두 가지 값의 비교가 가능하고 어느 한 가지 값에 가중치를 주어 계산할 수도 있는 방법이 있다.

3.2.1 손해 수준의 정의

기존의 위험 평가 프로세스에서는 손해 수준에 대한 언급이 부족하였으나 개선된 위험 평가 프로세스에서 손해는 위험을 결정하기 위한 가장 중요한 인자(factor) 중에 하나이다. 손해는 자산의 중요도나 가치로부터 유추된다. 손해는 자산의 중요도와 위험에 내재된 손해 속성을 평가하기 위해 동일한 규격을 사용하여 결정되고 이용되어야 한다. 보안의 3요소 중 비밀성에 손해를 입은 경우 그러한 손해 정도를 측정하기 위해 사용되는 손해수준의 예를 들면 다음과 같다.

- 특별히 중대한 영향을 미치는 손해 (ex. Top Secret)
- 중요한 영향을 미치는 손해 (ex. Secret)
- 영향을 주는 정도가 약한 손해 (ex. Confidential)
- 영향이 거의 없는 손해 (ex. Public)

무결성, 가용성, 혹은 재무적 영향 측정 중 한 부분에 국한하여 손해 수준을 이용하지는 않는다. 따라서 손해 수준은 무결성 손해, 가용성 손해 같은 손해의 여러 측면을 고려할 필요가 있다.

손해 수준은 TRR 결정 시 수준의 조합을 용이하게 하기 위해서 위험 수준과 동일하게 5가지 수준(Level)으로 나뉘어 표현(중요도/손해 0, 저, 중, 고, 매우 높음)되며 수준 별로 보안의 3요소인 비밀성, 무결성, 가용성이 손상될 시의 영향 정도를 기술하고 있다.

위험 수준을 결정하는 접근방식의 정량화를 통한 산출물의 정확성을 요구하는 프로세스는 조직 내 시스템에서 반드시 존재하고 이러한 필요성의 충족을 위해 손해 수준의 정량화는 반드시 필요한 과정이다.

재무적 손해는 구체적인 금액으로 측정되고 정확한 수치로 환산되는 것이 가능하기 때문에 파악이 어려운 경우(예를 들면 정보, 신용)를 제외하고 측정이 용이하다. 하지만 고려해야할 변수들 - 신용수준, 자본, 재정 상태에 영향을 미치는 자원, 이윤산출, 기업생존 - 이 상당히 많기 때문에 재무적 손실 계량화를 통한 효과 평가가 용이한 것은 아니다.

재무적 손실의 계량화 공식은 다음과 같다.

$$K=(Cp+Ct+Cr+Ci)-(I-A)$$

K : 총 손실 비용
Cp : 영구 교체 비용
Ct : 임시 교체 비용
Cr : 총 관련 비용
Ci : 수입 손실
I : 이용 가능한 보험이나 보상금
A : 적용 가능한 보험 프레미엄
[D.A. Stolovitch and L.D. Robertson]

위험 수준별로 재무적 손해는 다음과 같이 고려될 수 있다.

- Level 1: 이 수준에서 자원과 관련된 재무적 손해는 재정 상태에 영향을 미치지 못한다.
- Level 2: 이 수준에서 자원과 관련된 재무적 손해는 재정 상태에 영향을 미친다.
- Level 3 : 재무적 손해는 운영 유지를 위해 소요되는 기업의 주요 자본을 재조정해야 하는 결과를 발생시킨다.
- Level 4 : 재무적 손해가 발생할 경우 기업은 현재와 미래에 기업이 책임져야 할 재무적 책임을 다하기 위해 기업의 주요 구조를 재조정해야만 할 것이다.
- Level 5 : 5 수준에서 재무적 손해가 발생할 경우 기업은 도산할 수 밖에 없다.

3.2.2 위험 발생 확률의 적용

위험 발생 확률은 앞에서도 언급했듯이 이전 데이터 단독으로 산출될 수는 없는 문제이다. 따라서 두 가지의 이용 가능한 산출물이 있는데 그것은 관련 지식과 이전 데이터이다. 우발적인 위협에 대해서는 이전 데이터를 고려하고 계획적으로 발생하는 위협에 대해서는 이전 데이터와 함께 위협 에이전트의 능력, 위협 에이전트의 의도, 위협 에이전트의 현재활동, 위협 에이전트가 위협 사건을 발생시킴으로서 창출할 수 있는 이익 평가, 위협 에이전트가 위협을 발생시키기 위해 필요한 노력정도 평가, 목표분석(목표적합성, 타당성, 허용가능성)을 고려해야만 한다. 이러한 사항을 모두 고려하기에는 기존의 4가지 수준으로 분류된 발생확률수준으로 부족한 점이 많기 때문에 본 논문에서는 9 단계로 세분화된 개선된 발생확률수준을 다음과 같이 제시한다.

- 발생가능성 없음
- 발생가능성 불확실
- 무시할 수 있음
- 매우 낮음
- 저
- 중
- 고
- 매우 높음
- 최상

4. TRR과 RAC의 결정 방법

TRR은 크게 TLL(Target Loss Level)과 TPL(Target Probability Level)로 구성될 수 있다. TLL은 관리층이 허용할 수 있는 최상위 손해 수준이다. 그리고 TPL은 관리층이 허용 할 수 있는 최상위 발생 확률이다. 위험이 손해 수준과 발생 확률의 조합이듯이 허용 불가능한 정도를 결정함에 있어서 허용 불가능한 손해와 허용 불가능한 발생 확률이 허용 불가능한 위험을 구성한다.

4.1 TRR과 RAC 결정의 4 단계

1 단계 - TLL 결정

관리층은 민감도 평가 결과를 검토한 후에 민감도 평가의 내용을 승인하게 된다. 관리층의 승인 작업(예를 들면 책임 있는 관리자의 서명)이 완료된 후 자산의 가치 혹은 민감도는 조직 내의 모든 구성원에게 전달되게 되고 구성원들은 자산의 가치 혹은 중요도를 인식하게 된다. 각각의 자산들에 대한 민감도 수준 결정 결과와 정량화된 재무적 가치는 만약 자산에 위험 상황이 발생하여 야기될 수 있는 최악의 손해 사례를 고려하여 결정된 결과물이라고 할 수 있다. 따라서 특정 자산에 대한 전사적인 책임을 가진 현업 경영층과 함께 관련 사항을 분석하고 각각의 자산에 대해 관리층이 허용할 수 있는 최대치(TLL)를 결정해야 한다.

TLL은 자산에 발생할 수 있는 최악의 손해 사례라고 볼 수 있고 자산 민감도와 위험에서의 손해 수준(Level)에 사용되는 수준과 동일한 크기를 사용하여 표현되어야만 비교가 용이하다. TLL을 결정할 때 분석/고려되어야 하는 사항은 다음과 같다.

· 자산의 운영적 중요도와 가치를 표현하여 각각의 자산에 대한 최악의 손해 수준을 반영하여야 한다.
· 자산의 본질적인 보안 관심사를 언급하여야 한다.
· 허용 불가능한 위험을 결정하는데 있어 고려되어야 하는 사항은 다음과 같다.

→ 법적 요구사항
→ 응용 가능한 조직의 정책
→ 응용 가능한 산업적/전문적 표준 및 법
→ 자산을 재설치 및 교체할 수 있는 조직의 능력
→ 관리층의 위험 허용 한계
→ 역할/목표의 성공 여부
→ 업무의 생존 전략
→ 이상을 고려한 최악의 손해 사례
→ 재무상의 이윤 및 자원 효과성
→ 관리층의 개인적 상태 수준과 위험 허용 자세

만약 측정된 TLL 수치가 측정된 최악의 손해 수치 이상이면 관리층은 측정된 손해 수치를 기꺼이 받아들일 수 있을 것이다. 다시 말하면, 앞에서 TLL을 최악의 손해 수치와 거의 동일시하여 언급하였지만 TLL과 최악의 손해 수치의 차이점을 구분하여 설명하면 TLL은 좀더 관리층의 허용수준을 고려하여 그들의 입장을 대변하는 수치이고 최악의 손해 수치는 관리층의 입장을 배제하고 물리적인 상태를 계산한 수치이다. 따라서 TLL과 최악의 손해 수치는 동일할 수도 있지만 다른 외부적 요인에 의해 달라질 수도 있다. 따라서 의사 결정 시 두 가지 수치의 비교가 매우 중요하다.

2 단계 - TPL의 결정

이전 단계로 돌아가서 생각해보면 TLL이 측정된 최악의 손해 수치 이하인 경우 관리층이 측정된 손해 수치를 받아들일 수 없으므로 식별된 각각의 자산에 대하여 TPL이 결정되어야 한다. TPL을 필요로 하는 각각의 자산에 대하여 TLL보다 크고 최악의 손해 수준보다 작은 손해 수준을 허용 불가능한 손해 수준이라고 말할 수 있다. 각각의 자산이 가지는 허용 불가능한 손해 수준에 대해 관리층이 허용할 수 있는 최대 위험 발생 확률을 식별, 기록하면 그것이 TPL이고 위험 발생 확률에서 사용되는 수준과 동일한 크기로 표현되어야 한다. TLL을 관리층이 허용할 수 있는 최대의 손해 수준이라고 봤을 때 TLL이 최악의 손해 사례 이하라는 말은 최악의 손해 사례가 발생하면 관리층은 그러한 손해를 허용할 수 없다는 뜻이고 만약 최상위 손해 수준이 발생한다면 관리층은 허용 범위 외에 존재하는 그러한 손해를 관찰하는 것이 불가능할 것이다. 따라서 TLL에 대해서 TPL은 항상 최상위 수준(최고 위험발생 가능성 수준)을 가진다고 말할 수 있다.

3 단계-TRR 표현을 위해 TLL과 TPL 조합

손해 수준의 범위	비밀성 손해		무결성 손해		가용성 손해		재무적 손해
	손해수준	TPL	손해수준	TPL	손해수준	TPL	손해수준
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
TLL		최상		최상		최상	
중간 손해 수준							
최악의 손해수준 사례							

<그림4-1> TLL과 TPL 조합

각각의 자산은 비밀성 손해, 무결성 손해, 가용성 손해 재무적 손해의 4 가지 TLL을 갖는다. (b), (d), (f) 열은 모든 가능한 손해 수준을 포함할 수 있다. (c), (e), (g) 열은 각각의 가능한 손해 수준이 표시된 TPL을 포함한다. (h)열은 최악의

재무 손해 사례와 목표 재무 손해에 대하여 금전적 가치를 포함한다. TPL은 재무 손실과는 관련이 없다.

<그림 4-2>에서 TLL에 해당하는 열은 관리층이 허용할 수 있는 손해 수준을 나타낸다고 할 수 있다. 따라서 손해 수준은 비밀성에서 1 등급, 무결성과 가

용성에서는 2 등급으로 낮은 손해수준을 나타내고 있지만 발생확률은 상대적으로 상당히 높다는 것을 알 수 있다. 즉, 발생할 가능성은 높지만 조직에 대한 손해 정도는 상대적으로 낮다는 것을 의미한다. 이것은 재무적 손해의 실재 액수가 최악의 경우에 비해 약 10%에 해당되는 것을 통해 증명될 수 있다. TLL 이후의 열은 허용할 수 없는 손해를 나타내며 비밀성, 손해에서 볼 때 발생확률은 점점 낮아지지만 손해 수준은 증가하는 것을 쉽게 알 수 있다. 무결성과 가용성 손해에서는 손해 수준과 발생확률의 변화 폭이 작은데 그 이유는 다음과 같이 서술할 수 있다. 무결성은 일단 관리층의 허용 수준을 넘어선 경우 이미 무결성이 손상된 것이므로 정도의 변화가 다양하게 나타나는 것이 불가능하고 가용성의 경우는 일단 가용성이 침해되어 조직의 운영이 중단되었다면 그 상태에서의 변화는 허용 수준을 넘어선 초기와 차이점을 찾아 보기 힘들 것이다.

손해 수준의 범위	비밀성 손해		무결성 손해		가용성 손해		재무적 손해
	손해수준	TPL	손해수준	TPL	손해수준	TPL	손해수준
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
TLL	1	최상	2	최상	2	최상	450$
중간 손해 수준	2	중					
	3	저					
	4	최저					
최악의 손해수준 사례	5	극저	3	저	2	최상	4400$

<그림 4-2> TLL과 TPL을 조합한 TRR 표현의 예

4 단계 - 위험 허용 기준 설정을 위해 TRR 사용

IT 시스템이나 조직 전체가 많은 수의 특이한 위험에 직면함에 따라 명문화된 위험 허용기준(RAC)의 필요성이 인식되었다. RAC를 개발하기 위해서 위험 허용의 기본 논리를 이해해야 하는데 위험 허용의 기본 논리는 다음과 같다.

· 만약 손해가 TLL 이하이거나 손해가 TLL보다 크더라도 발생확률이 TPL 이하이면 위험이 허용 가능하고 아니면 불가능하다.

이전에 이미 TRR이 개발되었다면 TRR에 위험 허용 조건을 새로이 추가시켜야 한다. 정리해 보면 다음의 경우에 자산, 전체 IT 시스템, 조직을 위한 RAC는 인가되지 않은 파괴, 수정, 방해 노출, 제거의 위험을 허용한다.

· 비밀성, 무결성, 가용성, 재무 손해가 TLL보다 작은 경우
· 허용 불가능한 손해의 발생확률이 TPL보다 작은 경우

4.2 TRR과 RAC의 문서화 및 유지 보수

TRR과 RAC는 위험 허용치를 의사결정에 이용하는 경영층에 보고되기 위해 적절한 책임을 가진 현업 관리층의 승인(서명)과 명문화된 기록이 필요하다. TRR과 RAC 구문은 이해가 용이하고 조직의 역할/목표, 핵심능력/활동, 그리고 자산/자원 간의 복잡한 상호관계를 정확히 나열하여야 한다.

손쉬운 운영, 이해 그리고 사용을 위해 복잡한 TRR과 RAC 구문은 필요치 않다. 표 형식을 차용하여 표현하는 것이 모든 필요한 정보와 상호 관계를 가장 용이하게 압축하여 나타내는 방법이다. 적절한 관리자에게 승인된 TRR과 RAC를 기반으로 목표(Target)가 정의된다. 목표를 기반으로 위험평가가 실시되고 위험평가 프로세스의 실시 과정에서 환경의 변화가 요구될 경우 요구사항 충족을 위해 실시 방법 조정이 필요할 수도 있다. 이때 TRR과 RAC는 참조할 수 있는 좋은 이정표가 된다.

결정된 TRR과 RAC가 현실적으로 적용 불가능할 경우 보안 실무자와 상부 관리층은 협의를 통하여 결정 사항을 적절히 수정해야 한다.

TRR과 RAC, 가용시간, 가용자원은 위험평가 프로세스를 이용한 보안 해결책 개발 시 제약사항이라고 할 수 있는데 TRR을 해결하면서 시간과 예산의 허용 범위 내에서 해결책을 개발하는 것은 거의 불

가능한 일이다. 이러한 경우 관리층은 보안 해결책에 더 많은 시간/자원을 투입하거나 더 높은 위험 수준을 허용하는 방향으로 TRR과 RAC를 수정함으로써 허용정도를 변경해야만 한다. 보안 실무자는 결정된 TRR과 RAC가 적절한 관리자의 의사결정과 승인을 통해 산출된 결과물임을 항상 염두에 두고 실시 방법 변경을 고려해야만 한다.

TRR과 RAC는 주기적으로 검토되어야 하고 위험 환경에서 변화가 필요한 경우 교정되어야 한다. TRR과 RAC가 교정되어야 할 경우는 다음과 같다.

- 조직의 역할/목표에 중요한 변경 사항이 생길 경우
- 위협 환경에 중요한 변화가 생길 경우
- 구체적인 업무/보안 이슈에 대하여, 입법· 산업 혹은 전문 표준의 변화나 자연적으로 증가하는 위험의 회피를 위해 혹은 위험 허용과 관련하여 조직의 정책 변경이 결정될 경우

5. 결론

TRR/RAC는 자세하고 구체적으로 정의된 목표(Target)라고 말할 수 있고 이를 통해 위험 평가 프로세스의 변환이 필요하게 된다. TRR/RAC 구문을 통해, 분석 노력의 효율성 개선, 작업 경로 단축, 분석에 소요되는 시간과 자원을 축소시킬 수 있다. 구체적이고 집중적인 분석 범위에 TRR/RAC를 사용하면 시간, 자본, 인력의 낭비를 방지할 수 있다.

관리층에 대한 보안 해결책 관련 보고 업무 수행 시 TRR/RAC를 제출하여 검토하도록 하고 검토를 통해 관리층에게 목표(Target)을 인식시킬 수 있다. 권고사항과 운영상의 시간/자원 및 비용 효과 보고가 가능하다. 보안 권고사항에서 추출되는 잉여 위험에서 본질적 위험과 최악의 손해 사례를 비교하는 것이 가능하다. 권고사항에서의 잉여 위험과 TRR을 비교하고 어떻게 권고 사항에서 TRR이 처리되는지 보고할 수 있고 권고사항을 정당화시키기 위해서 비용 이익 및 투자대비 회수율을 사용할 수도 있다. 관리층이 객관적/독립적이라면 자산 중요도/가치와 TRR/RAC 결정에서 그들의 참여가 중요함을 인식시킨다. 관리층에서 결과에 만족하지 않을 경우, 그들이 허용할 수 있는 부가적인 위험을 식별하여 목표(Target)를 다시 제시할 것을 요청하고 만약 TRR/RAC가 변경될 경우 적절한 관리자의 승인을 받고 결과를 문서화한다.

논의 자체가 세부적인 전술상의 수준 평가를 취급하고 조직의 자산/자원에 발생할 수 있는 위험에 근간을 두기 때문에 전술상의 수준 평가가 가능하다. 운영적인 수준에서 보면 자산 대신에 조직의 업무 능력과 활동에 기초하여 TRR/RAC를 결정한다. 전술상의 수준평가보다는 상세함이 부족하지만 TRR/RAC의 운영적 수준 정의는 세부적인 전술상의 TRR/RAC 수준 정의의 지침이 된다. 전략적 수준에서 보면 상업성을 띈 조직이나 정부 부서를 대상으로 TRR/RAC를 결정하고 이러한 평가의 수준은 조직의 역할/목표에 초점을 두고 있고 운영적 수준 평가보다 더욱 일반적이다. TRR/RAC의 전략적 수준 정의는 운영적인 TRR/RAC 수준 개발의 지침이 된다.

이외에 IT에 관련하지 않고도 물리적 보안, 구성원 보안, 보안비상계획관리, 보안과 계약관리, 정보보안(비IT), 운영보안(비IT), 통신 보안 등에 TRR/RAC는 응용이 가능하다.

본 논문에서 제시한 TRR과 RAC 결정 및 처리 방법론을 이용하면 위험관리자와 상부 관리층의 수평적 의사소통이 가능하게 됨으로써 이러한 문제점을 해결할 수 있다. 그리고 TRR이 결정되어 위협 및 위험 평가 프로세스의 기본 자료로 이용됨으로써 위험의 처리와 대비책 구현에 효율성을 재고할 수 있다. 따라서 TRR을 통해 조직이 얻을 수 있는 장점을 종합적으로 기술해 보면 크게 다음의 네 가지 사항으로 분류할 수 있다.

- TRR은 시간과 작업 비용의 절감 뿐만 아니라 위험 평가의 효율성과 효과성을 개선시킨다.
- TRR은 최고 경영진에게 위험 허용 기준을 제시한다.
- 권고사항을 통해 최고 경영진의 지원과 구현 동의를 얻어낼 수 있다.
- IT 시스템과 조직 전체에 보안 인식을 재고시킨다.

Reference

(1) Amit Yoran and Lance J. Hoffman, Role-Based Risk Analysis, George Wasington University Cyberspace Policy Institute, 1995, p 589

(2) D.A. Stolovitch and L.D. Robertson, How to Determine and Use Target Residual Risk, Ottawa Congress Centre, June 1998

(3) Donald R. Peeples, Infosec Risk Management: Focused, Integrated & Sensible, National Security Agency, 1995, p578~579

(4) Geoffrey H. Wold and Robert F. Shriver, Risk Analysis Techniques, Disaster Recovery Journal, 1997

(5) Hilary H. Hosmer, New Security Paradigm: Orthodoxy and Heresy, Data Security, Inc. 1996, p69~73

(6) ISO/IEC TR 13335-3, Information Technology-Guideline for the Management of IT Security-Part 3: Techniques for the Management of IT Security, Technical Report, June 1998

(7) Joan Fowler and Robert C. Seate III, Threat and Vulnerability For C4I in Commercial Telecommunications : A Paradigm For Mitigation, Data System Analysts, Inc. 1994

(8) Judith L. Bramlage, A New Paradigm For Performing Risk Assessment, Computer Associates International, Inc. 1996

(9) Marian H. Long, Business Interruption Risk Assessment: A Multi-Disciplinary Approach, Disaster Recovery Journal, 1997

(10) RCMP, Guide to Threat and Risk Assessment For Information Technology, IT Security/Securite des TI, November 1994