기업의 사업 연속성을 고려한 통합 보안관리 기능에 관한 연구

남상훈*, 임종인**
*SKTelecom, swnam@sktelecom.com
**고려대학교, jilim@korea.ac.kr

A Study on Function of Total Security Management based on Enterprise Business Continuity

Sangwhun Nam*, Jong-in Lim**
*SKTelecom, Seoul Korea
**CIST, Korea University

요 약

본 연구는 기업의 사업연속성 확보를 위한 관점에서 정보보호 영역의 통합보안관리 기능을 확장, 제시한다.
기업은 윤리경영을 기초로 사업과 서비스를 통한 수익창출을 목적으로 하며, 기업이 사업의 중단을 가져올 여러 요인을 사전 파악하여 예방, 대응하는 것은 기업의 생존에 직결된다. 기업의 사업연속성에 관련된 요인은 다양하고 복합적으로 관련되어 있어 조기 파악하고 관리하는 것은 어려운 일이다. 그러므로 사업연속성에 영향을 미치는 위험 요소에 대한 기능들이 개별적으로 운영되기 보다, 종합적으로 연계되고 일관적으로 관리되어지는 것이 필요하다.
대부문의 기업이 자사의 사업 및 서비스를 정보화에 의한 정보통신 및 정보처리 환경에서 운영하고 있어, 주요 경영정보 및 고객정보의 유출 및 해킹으로 인한 보안사고는 기업의 사업연속성에 점점 심각한 영향을 미치고 있다.
종합적인 보안관리를 위한 통합보안관리의 기능은 매우 중요하나, 현재 정보보호의 범위안에서 보안관제를 주 기능으로 활용하고 있으며, 구축된 보안관리 기능도 제한적으로 활용되고 있는 상황이다. 그러므로, 사업연속성 확보를 위한 기업의 통합보안관리 기능과 환경에 대한 개선 및 재검토가 요구된다. 이를 위해 사업연속성 확보를 고려한 통합보안관리의 기능항목과 구성을 정의하고 통합보안관리의 추진 방향과 기 구축된 통합보안관리 환경의 개선사항을 제시하여 통합보안관리가 기업의 사업연속성 확보에 실질적인 역할을 하게 함에 있다.

1. 서론

우리가 살아 가는한 위기는 존재한다. 위기는 관리의 조건에 따라 위험적이거나 발전적 상황으로 전개 되어질 수 있다. 그러므로 현상에 대해 체계적인 예방과 관리를 하므로써, 문제요인을 사전제거하고 긍정적인 방향으로 예측 가능하게 만들어 가야 한다.
기업의 존재 이유는 윤리적인 경영하에서 수익 창출을 통해서 인류사회에 기여함에 있다.
기업의 수익창출을 위해 내, 외부의 재난을 사전 예방하고 발생시 신속하고 대응하는 체계를 갖추는 것은 기본적인 전제가 된다. 그리고 대부분의 기업의 사업과 서비스가 정보처리를 기반으로 하고 있는 상황에서 과거의 단순한 사고에서 탈피하여 점점 복합적이고 고도의 기술을 배경으로 하여 발생되는 재난의 성격으로 변해가고 있다.
특히 유,무선 통신과 IT 환경의 발달로 기업의 존립에 영향을 미치는 핵심기술과 고객 및 경영정보에 대한 해킹과 유출의 가능성은 급격히 높아지고 있다.
그러므로, 기업은 이에 대응하여 전사적인 시각에서 관련된 Risk 들을 인식하고 종합적인 관리를 통해 일정한 허용 한계내에서 적절하게 관리하는 것이 필요하게 된다. 통합보안관리는 정보보안 영역에서 단위 보안기능의 일관적인 관리와 중앙 집중형의 관제 및 보안정보의 공유를 통해 회사의 정보자산을 사, 내외 보안 공격과 사고로 부터 안전하게 유지, 보존하기 위한 목적으로 구축된다. 그러나 현재 다수의 통합보안관리의 적용현황은 보안관제기능을 중심으로한 제한적인 기능으로 운영되고 있다. 통합보안관리는기업의 사업연속성을 고려, 전사 Risk 관리 체계와 연계하여 요구기능을 고려, 반영되어져야 한다.

통합보안관리 기능은 기업의 Risk 관리 체계와 함께 정보보호 운영과 관리 기능외에, 정책과 투자결정에 관련되는 경영층에 시스템적 지원을 염두에 두고 구축, 활용되어져야 한다.
특히 IT 환경에서의 보안사고의 발생으로 인한 장애 및 재해는 신속하게 전개되는 점을 고려, 사업연속성에 심각한 영향을 미칠 수 있는 전사적인 Risk 관리기능과의 정보공유 및 연계처리 역할을 하여야 한다.

2. 기업의 RisK 와 사업연속성

2.1 Risk 증가와 기업의 Risk

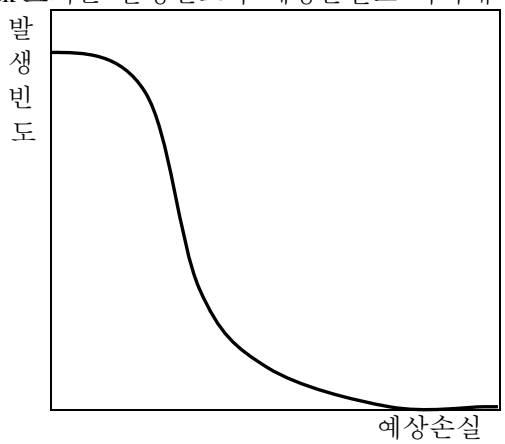
자연과 인간의 관계, 그리고 인간 사회의 복잡도에 비례하여 Risk 의 영향과 심각함이 증대되고 있다.
현실적으로 기업은 재무영역외에 IT, 영업, 인사, 윤리 등의 다양한 부문에 위험의 요소를 가지고 있다. 재난의 유형은 <표 1>과 같이 분류될 수 있으며, 정보사회에서 빈발하는 재난은 대개 복합-돌발형의 특징을 갖는다. 허브나 커넥터에 해당하는 서버가 공격받을 경우에 순식간에 그 피해가 전체 네트웍크로 확산될 수 있는 가능성이 크기 때문이다. 현대 사회는 각종 금융거래, 주식의 매매, 온라인 예약시스템과 사이버거래 등이 복잡하게 맞물려 있는 상태에서 네트워크 환경의 돌발적인 와해는 상상하기 힘든 피해를 가져올 수 있다.[1]

<표 1> 재난유형 분류

상호작용 \ 사건의 소요시간	길다	짧다
복잡	복합-중복형 (환경오염 재난유형) 러브케넬 사건 LA 스모그	복합-돌발형 (고도기술 재난유형) 첼렌저 폭발,보팔참사 인터넷대란
단순	단순-증폭형 (단순기술, 부실유형) 삼풍백화점/성수대교붕괴, 그랜드 테턴댐 붕괴	단순-돌발형 (단순사고, 범죄유형) KAL 기 폭파 자동차사고 등

2.2 Risk 의 평가와 관리

기업에 영향을 미치는 Risk 요소들은 수립된 합리적이고 객관적인 기준에 의해 평가되고 관리되어야 하며 Risk 크기는 발생빈도와 예상손실로 나타내 진다.



(그림 1) Risk 발생빈도와 예상손실 관계 [2]

Risk = (사태의 가능성) * (사태의 결과)
= (사태가 일어나기 쉬운 확실성의 정도) * (사태의 발생에 따른 피해)

2.3 Risk 분석과 사업연속성, 전사적 위험관리

기업의 Risk 는 계층별로 분류되고 체계적인 분석을 통하여 기업이 직면하게 되는 경영위험 등을 포함한 다양한 위험에서 사업연속성 확보가 필요하다. 그리고 전사적인 시각에서 통합적으로 인식하고 관리하는 새로운 위험관리가 요구된다. 특히 기업의 조직시스템의 Risk 는 계층별로 전략적인 관점에서 전략점 위험, 프로세스 관점에서 업무 위험, 자원복구관점에서 운영적 위험으로 구분할 수 있다. Risk 관리는 조직의 재해, 장애 등 손실을 최소화시키기 위한 절차 혹은 연속적인 행위(위험의 분석, 평가, 대책 등)이다. 이러한 조직의 일반적인 위험을 통제할 수 있는 Risk 관리는 조직내의 대부문의 업무가 정보기술에 의존되어 있으므로 크게 업무연속성관리와 정보기술서비스관리로 구분할 수 있다.

(그림 2) 조직 시스템의 위험계층 구조 [3]

3. 정보보호 영역에서 통합보안관리

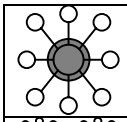
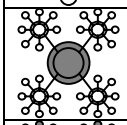
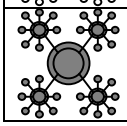
3.1 통합보안관리의 목적과 유형

통합보안관리는 일괄적인 보안관리와 보안관제, 보안 Solution 의 운영 및 보안정보 공유 등의 기능을 통해 투자 효과대비 보안예방과 신속한 대응활동을 가능하게 하여 조직의 보안수준을 향상시켜갈 수 있다. 기업은 통상 통합보안관리를 통해

1) 중앙 집중식, 포괄식, 통합식 관리의 실현
2) 일관된 보안 정책 실현
3) 보안 관리 비용 절감
4) 적은 인원의 정보보안 전담인력을 이용한 효과적인 보안통제를 효과적으로 추진할 수 있으며
5) 통합 정보보안 기능에 의한 정량적 효과로

보안침해사고 해결능력향상(약 20~25%)과 사용자/관리자 비율의 증가(약 20%)와 보안침해사고시 업무중단시간 감소(50%)를 얻을 수가 있다. (ICSA Information Security 2000.9)

통합 보안관리 유형은 Local, Remote, Complex 관리 형태로 나누어 정의해 볼 수 있다.

	Local 관리 -보안 관리 대상들에 대하여 직접 통합보안관리 시스템으로 연동하여 Monitoring 및 Control & Management 수행
	Remote 관리 -보안 관리 대상에 대하여 로컬 별로 연동하고, 중앙의 통합보안관리 시스템으로 중앙에서 전 지역을 통합하여 일괄 관리
	Complex 관리 -보안관리 대상들에 대하여 직접 통합보안관리 시스템으로 연동하고 각 지역의 관리자와 중앙 보안 관리자 역할

(그림 3) 통합보안관리 유형

3.2 통합보안관리 기능

통합보안관리는 보안Event의 분석보고, 보안관제, 보안관리, 보안정책 관리 및 단위보안솔루션의 운영기능 등을 기초로 종합적인 보안현황을 관리하게 된다. 통합보안관리는 정보보안 솔루션들을 기술적으로 통합 연동하여 one-point management 가 이루어 질 수 있도록 하며, 기술적인 각종 네트워크 보안제품의 통합관리와 개별 침입에 대한 종합적인 대응이 가능하도록 각 제품간 인터페이스 및 교환되는 메시지 포맷을 표준화하여 모니터링과 원격지 중앙관리까지 가능한 지능형 보안관리 시스템으로 관리하는 것이 가능하다. 그리고 현실적으로 기업내 보안조직의 성격과 특성에 따라 통합보안관리가 상이하게 정의되고, 다양하게 운영되고 있다.

조기 예,경보의 기능을 보안관제 내에 정의하여 기본기능으로 두는 경우도 있으며 기존의 통합보안관리에 추가되는 별도의 기능군으로 정의하기도 한다. 후자의 경우는 사전 통합보안관리에 사전 조기 예,경보 기능을 정의하고 구축된 시스템이 아닌 경우에 그러하다.

3.3 통합보안관리의 변화

통합보안관리 기능도 점진적으로 개선되어 가고 있으며 여러관점에서 변화를 정의할 수 있는데, 보안관제를 중심으로 다음과 같은 단계적으로 나누어 볼 수 있다. 1 단계는 통합보안관리로 모니터링하면서 매일 수천건, 수만건의 많은 이벤트가 발생의 되는 상황에서 일정한 방법으로 필터링하여 관리자가 연관관계나 사고대응 등의 업무 처리를 수동적인 기능으로 처리한다.

2 단계는 데이터의 대규모 발생으로 분석이 불가능했던 1 단계에서 보다 발전하여, 정보보호정보 혹은 이벤트간 연계분석, 상관관계분석, 분석결과의 전파와 대응을 수행하고 있지만, 역시 아직은 많은 양의 데이터와 분석 근거 부족으로 실시간 침해사고 대응, 공격평가, 조기예,경보 등의 대응이 이루어 지지 못한다.

3 단계는 데이터마이닝 등을 통한 정보 상관분석, 침해사고 분석 시스템구축, 사고 예방기능 강화, 블랙리스트에 기반한 공격 대응, 시각화, 역추적 시스템기술 등을 목표로 하고, 필요시 시스템적인 조기경보와 대형 관제센터간에 실시간 정보공유가 필요한 조기경보 네트워크가 구축되어 제공된다. [4]

4. 사업연속성 확보를 고려한 통합보안관리 기능

4.1 사업연속성 확보 고려 요소

기업의 사업연속성을 확보 지원하기 위해 통합보안관리에 고려되어야 할 주 요소는 기업에서 수립된 사업연속성 확보 기준과 이를 기초로 심각한 영향과 Risk 가 발생될 수 있을 때 체계적으로 탐지된 결과를 기초로한 보고체계 등을 중심으로 정리해 볼 수 있다.

1) 보안정책과 보안안정성 및 서비스 확보 기준
   - 보안 SLA 및 보안서비스 Baseline
2) 보안관제에 의한 Event에 의한 보고체계
3) 조기 예,경보 기준 및 관리
4) 보안Event의 정규화된 Data를 이용한 통계관리와 이를 통한 투자대비효과 분석결과 관리
5) 전사 Risk관리 체계와의 연계, 관리방안

4.2 전사적 Risk 관리와 통합보안관리

전사적 Risk 관리는 기업이 직면한 Risk 에 대한 전체적인 시각을 제공하는 한편, 재무적인 대안과 조직적인 대안을 효과적으로 혼합하여 최적의 위험관리 대안을 도출해 낸다. 전사적 Risk 관리를 기반한 통합보안은 전사의 보안업무를 통합하여 관리할 수 있는 Portal 기능으로 진화하여야 한다. 즉, 사내의 제도적 보안 준거 현황, 주요 자산들에 존재하는 기술적인 취약점 현황, 물리적인 보안 현황을 모니터링 할 수 있어야 한다. [5]

특히, 미국의 비정부 기구인 COSO(the Committee of Sponsoring Organizations of the Treadway Commission)가 2003 년 7 월 발표한 ERM Framework 을 기초로 통합보안관리와의 관계를 정의하고, 연계기능 및 관련 처리를 고려하는 것이 바람직 하다.

<표2> COSO Risk Framework과 통합보안관리

ERM(Enterprise Risk Management)			
ERM Benefit	ERM Definition	ERM Components	Role & Responsiblity
o 내부 위험관리 환경 o 목표 설정 o 위험요인 인식 o 위험평가		o Risk 대응 o 통제 활동 o 정보 및 커뮤니케이션 o Monitoring	
↕			
TSM(Total Security Management)			
보안관리	보안관제	보안기능 운영	보안정보 공유

기업에 수립되었거나 수립될 전사 Risk 관리체계의 Components 를 고려하여 통합보안관리 기능에서 생성, 유지하여야 할 정보의 성격과 상세 정의가 필요하다.

4.3 기업 사업연속성을 고려한 통합보안관리 기능

사업연속성 확보 고려요소를 기초로 통합보안관리의 내부 정책기준, 관리체계의 강화와 외부 Risk 관리와의 연계기능의 중점적인 관리가 필요하다.

1) 보안관리

각종 보안 정보를 토대로 보안 현황에 대한 분석 및 통계정보의 관리가 요구되며 보안정책의 적용과 통합보안에 대한 정책수립 및 관리 그리고 전사적 지원,연계 기능이 필요하다. 이를 위해 자산 관리, 정책 관리, 구성 관리, 성능 관리, 장애 관리, 이력 관리, 보안투자 관리, 무결성 관리, 스케쥴 자동관리의 통계분석과 보안서비스에 대한 SLA 의 기준에 의한 평가항목과 사내 전사 Risk 관리 기능 및 아웃소싱 환경에서 R&R 의 명확한 정의를 한다.

2) 보안정보 공유

전사 대상의 보안 관련 정보에 대한 효율적인 수집과 유지, 공유 그리고 유용한 보안정보의 지속적인 수집과 분석, 통계화 기능이 필요하다. 이를 위해 보안현황, 보안관리, 보안운영/관제, 침해사고 예방 및 대응, 보안 커뮤니티와 연계될 전사 Risk 관리체계에 공유할 정보항목과 보안 Reference 정보가 요구된다.

3) 보안관제

실시간으로 보안, 이벤트및 보안솔루션의 모니터링 업무 수행,식별,추적,대응 및 365 일 24 시간 무정지 관제의 지원 기능이 필요하다. 이를 위해 전문적 관제기준, 관제 모니터링, 로그 관리, 이벤트 관리, 자동대응, 조기예/경보, 장애관리, 보고 항목이 요구된다. 조기예,경보가 별도 기능군으로 정의될 경우 Interface 관리 항목을 필요로 한다.

4) 보안기능 운영

단위 보안 솔루션의 운영 상태를 감시 및 설정과 보안 솔루션에 대한 단계적인 연동, 성능 및 확장관리 방안에 기초한 연동기능이 필요하다. 이를 위해 단위 보안기능별 설정 및 차단, 탐지 및 복구 등 운영현황, 처리, Feedback 정검 항목을 정의한다.

<표 3> 통합보안관리 기능구성

<table>
<tr><td rowspan="15">통합보안관리</td><td rowspan="5">보안관리</td><td>정보보안정책</td><td>보안통계분석</td><td colspan="2">보안조직/R&R</td></tr>
<tr><td>사규,정책,지침,
보안서비스
기준 및 SLA</td><td>자산,구성,성능
장애,이력,투자
등보안통계/분석</td><td colspan="2">보안조직현황,
전사 Risk 관리
조직과의 R&R</td></tr>
<tr><td colspan="4">전사 Risk 관리체계 연계,</td></tr>
<tr><td>자산분석</td><td>타당성분석</td><td>위험분석</td><td>실행방안</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="2">보안정보공유</td><td colspan="3">보안 Issue 정보</td><td>전사 Risk 정보</td></tr>
<tr><td>보안솔루션,
동향/ 상황정보</td><td colspan="2">통합보안
로그/이벤트</td><td>Risk 관련
침해/ 대응정보</td></tr>
<tr><td rowspan="5">보안관제</td><td colspan="2">보안현황 분석</td><td colspan="2">보안분석 보고</td></tr>
<tr><td>시스템별
사고현황</td><td>침입유형별
사고현황</td><td>시스템,
NW 보안
정보관리</td><td>침해사고
보고 및
이력관리</td></tr>
<tr><td colspan="2">보안관제</td><td colspan="2">침해사고</td></tr>
<tr><td>보안시스템
운영현황</td><td>보안관제
현황</td><td>침해사고
예방</td><td>침해사고
대응</td></tr>
<tr><td colspan="4">조기 예/경보</td></tr>
<tr><td rowspan="4">보안기능운영</td><td>Application
& Data</td><td>System &
Platform</td><td>Network</td><td>OA</td></tr>
<tr><td>차단</td><td>시스템
침입차단</td><td>Network
침입차단</td><td>OA
침입차단</td></tr>
<tr><td>탐지</td><td>서버
침입탐지</td><td>Network
침입탐지</td><td>OA
침입탐지</td></tr>
<tr><td>Feedback</td><td>시스템
장애복구</td><td>Network
경로복구</td><td>OA
보안복구</td></tr>
</table>

5. 결론

기업의 사업연속성 확보를 고려한 통합보안관리는 전사적 위험관리의 객체와 연계, 관리되어야 하며 발생정보를 기초로 통계 및 영향이 분석되어야 한다. 그리고, 정보보호와 관련된 사회적인 현상이 어느 정도 정규화되고 이에 대한 자료가 점차 축적됨에 따라 정보보호에 대한 경제학적 접근과 같은 정량적 처리가 중요하게 되고[7], 통합보안관리에 적용과 활용이 필요하다.

통합보안관리는 정보보호 영역을 중심으로

1) 통합보안관리의 종합적인 정책기능과 상위의 사업연속성 관련 체계와 맥을 같이해야 한다.
그리고, 기업내 통합보안기능에서 관리되는 보안정보의 통계분석을 통해 보안정책의 수립과 경영층의 의사결정과 관련한 지원기능을 갖어야 한다.

2) 조직내 역할 정의를 기초로, 타당한 정보의 관리가 전사적 위험관리에 기반하여 구성, 구축되어 사업연속성의 대상요소를 파악, 분석을 통해문제에 접근해 가는 것이 요체가 된다.

3) 보안기준과 서비스에 대한 기업내 및 기업외의 아웃소싱환경을 반영한 SLA 과 서비스 Baseline 의 수립과 적용방안이 통합보안의 보안관리기능내에 정의되어 적용되어야 한다.

4) 통합보안관리의 전사적 영향 및 파급효과를 고려하여 보안영역을 중심으로 조직 특성과 환경을 반영한 지속적인 개선 체계를 수립하고 점차적으로 종합적인 기능으로 개선시켜가는 것이 필요하다.

5) 정보보호 활동의 정규화된 정보를 기초로, 객관적인 평가, 통계적인 관리기능 강화를 통해 정보보호 정책 및 투자결정에 지원, 활용되어져야 한다. 통합보안의 종합적인 결과를 조직이 보안조직에서 관련된 총괄조직으로 기능이 수렴되고, 체계가 정의되어야 한다.

그리고 통합보안관리는 특성상 단편적인 문제해결보다 종합적인 문제관리에 촛점을 두고 개선시켜가는 것이 타당하다.

참고문헌

[1] 이재열(2004) "위험사회와 정보화의 명암"

[2] 이영재, 윤정원(2003) "BCP 입문, An Introduction to Business Continuity Planning", 디지털타임즈

[3] 김기윤(2004) "정보보호를 위한 장애관리의 위험평가"

[4] 최운호(2004) "대규모 사이버 공격에 의한 침해사고 대응시스템 자동화 모델 설계"

[5] 김종호(2004) "전사적 위험관리: 개념과 사례", LG 경제연구원

[6] 주진오, 이성수, 이영재(2004) "ITA/BCP Working Together", 동국대 위기관리연구센터

[7] 신일순(2004) "정보보호의 경제학적 의미에 대한 소고"