Executive Series

CIO가 염두에 두어야 할 보안의 핵심

"긍정의 부서"로 거듭나기

주요 내용:

기업이 혁신의 기회를 놓치지 않으려면 IT 보안의 문화가 "부정(No)"에서 "긍정(Yes)"으로 진화해야 합니다. IBM은 실용적, 긍정적, 전략적으로 IT 리스크를 관리할 수 있도록 보안 조직을 5개의 핵심 기능 영역으로 변혁하였습니다.

귀사에서 가장 중요한 업무가 무엇인지 잠시 생각해 보십시오. 전 세계에서 금융 거래를 수행하는 것일 수도 있고, 한 도시의 전력 공급을 제어하는 것일 수도 있으며, 승객 수백만 명의 항공권 예약을 처리하는 것일 수도 있습니다. 그러한 업무를 총괄하는 컴퓨터가 해킹 당하거나 작동을 멈춘다면, 고객이 거래를 할 수 없거나 전 세계의 항공권 예약 정보가 사라진다면 비즈니스에 어떤 일이 발생하겠습니까? 이처럼 끔찍한 상황이 일어날 수 있기 때문에 많은 정보 보안 책임자들은 기존의 시스템을 그대로 유지하려고 하며, 정교하게 안정성을 유지하고 있는 보안 운영에 위협을 끼칠 수도 있는 이니셔티브는 거부합니다.

IDC/RSA의 연구 조사에 따르면, 보안 문제가 혁신을 저해하고 있다고 합니다. 2008년도 설문에 참여한 기업 임원의 80% 이상이 정보 보호에 대한 우려 때문에 혁신적인 비즈니스 기회를 추진하지 못한 경우가 "가끔" 또는 "자주" 있었다고 밝혔습니다.[1] 최근 조사에서도 보안 문제는 소셜 기술과 전자 의료 기록에서부터 열린 정부 플랫폼과 스마트 그리드 기술에 이르는 여러 혁신적인 기술의 도입 속도를 늦추는 요인으로 지목되었습니다.[2] 많은 기업에서 IT 보안 조직은 새로운 아이디어를 무산시키고 방해하는 악역을 맡으면서 "부정(No)의 부서"로 인식되고 있습니다.

이제는 변화가 필요합니다. 보안 조직은 기업 운영의 영역까지 그 역할을 확대함으로써 보안 과제에서 중점적으로 해결해야 할 영역을 확실히 하고 적절한 대응을 할 수 있도록 계획하여 새로운 아이디어나 이니셔티브를 수용해야 합니다. 이러한 변화를 위해서는 포괄적이고 체계적인 방식으로 보안에 접근해야 하며, 이를 뒷받침할 조직 구조도 필요합니다.

IBM은 이러한 것들을 구현해냈고, 그 과정에서 보안 팀은 "긍정(Yes)의 부서"로 변모할 수 있었습니다. 장기간에 걸쳐 경영진의 리더십 하에 개발된 이러한 접근방식은 보안 분야에 희망의 빛을 비췄으며, 이와 함께 조직의 변혁도 실현되었습니다.

이 글에서는 IBM의 경험을 토대로 기업 보안을 위해 실용적이고 발전적인 조직 구조를 정착시키기 위한 5가지 기능을 간략하게 소개합니다. 이 기능들은 혁신과 리스크 사이의 균형을 유지할 수 있도록 하며 부서의 문화를 "부정(No)"적인 것에서 긍정(Yes)"적인 것으로 바꿔줍니다.

1. 정의

첫 번째 기능은 조직이 3~5년까지 내다보는 미래 지향적인 전략을 가지고 IT 리스크를 해결할 수 있도록 집중하는 것입니다. 이것은 어떻게 가능할까요? 실제로 이러한 조직은 새로운 이니셔티브 또는 환경의 변화를 염두에 두고 비즈니스 측면에서 기존 및 새로운 IT 리스크에 관한 정보를 수집하고 이 리스크가 효과적으로 관리되는지 판단할 것입니다. 이 기능이 제대로 수행된다면 "방향을 수립"할 수 있으며 방향 수정이 필요한 지점과 시점을 파악할 수 있습니다. 가장 중요한 것은 이러한 활동을 통해 리스크 관련 지출을 투자로 다룰 수 있다는 점입니다.

주요 리스크 시나리오:

사이버 보안	보안 공격 또는 바이러스 감염에 의한 데이터 센터 마비, 영업 기밀 누설, 고객 데이터 유출
IT 컴플라이언스	고객 데이터의 잘못된 취급과 같은 규정 위반으로 인한 업무 차질 및 이미지 실추
공급망	기술 공급업체의 문제로 계약상 의무 불이행 및 서비스 중단
비즈니스 혁신	전략적 기술 프로젝트의 지연, 예산 초과 또는 운영상의 문제

[1] "Innovation and Security: Collaborative or Combative", IDC(RSA 의뢰), 2008년 9월
http://www.rsa.com/innovation/docs/IDC_innovation.pdf

[2] "HP and AMD Research Shows Concerns about Security, Technology Budgets Are Main Barrier to 'Gov 2.0'", 2012년 4월 24일
http://www.hp.com/hpinfo/newsroom/press/2012/120424c.html

2. 계획

이 역할은 정책 및 아키텍처 팀의 몫입니다. 규모가 작은 기업에서는 전략 팀에서 이 역할을 맡기도 하며, 이 전문가들은 앞으로 수행할 단계를 계획합니다. 기술과 공급업체를 파악하고 예산과 일정을 편성합니다. 즉, 전략적 목표를 실현하기 위한 계획을 수립합니다.

각각의 보안 기능이 지속적인 발전의 기회를 제공하므로, 피드백 루프를 개발하는 것이 필수적입니다.

3. 구현

이제 관리 팀은 이 계획을 실천해야 합니다. 예를 들어, 바이러스 방지 프로그램의 경우 특정 시스템 전반에 설치합니다. 이와 동시에 자신들이 수행하는 단계를 서비스 카탈로그에 등록합니다. 그러면 설치된 툴을 다시 사용할 수 있습니다. 오류가 발생한 경우에는 세부적인 기록을 통해 분석을 할 수 있습니다.

4. 측정

컴플라이언스 전문가는 현재 마련된 통제 기능의 실효성을 분석합니다. 이들은 보안 목표가 달성된 부분은 어디이며 미진한 부분은 어디인지를 파악합니다. 또한 악성 코드 감염률과 같은 주요 리스크 지표를 확인하고 균형성과기록표(Balanced Scorecard)에 조사 결과를 상세히 기록합니다. 이는 분기마다 전략 팀에게 전달됩니다.

5. 대응

아무리 꼼꼼하게 계획하고 준비를 하더라도 문제가 생길 수 있습니다. 바로 이때 사고 대응 팀이 나섭니다. 위기 상황에 대응하는 과정에서 이들은 문제점에 대한 중요한 정보를 얻습니다. 이 피드백은 전략 팀에 전달되어 기술 및 정책 구성 요소 개선을 위해 쓰입니다.

IBM CIO—IT 리스크: 기능적 조직

각각의 기능은 지속적인 발전의 기회를 제공하며, 이를 위해 피드백 루프를 개발하는 것이 중요합니다. 이를테면 전략 팀은 균형성과지표를 분석하여 해결되어야 하거나 개선이 필요한 영역을 찾아냅니다. 따라서 기술 통제의 효율을 높이거나 정책 요구 사항을 명확히 하거나 직원의 보안 인식 제고 프로그램에 투자하는 것이 필요하게 됩니다.

성공의 관건 중 하나는 정보 보안 책임자가 임원 회의에 참석하는 것입니다. 2012년 IBM 최고 정보 보안 책임자 평가에 따르면, 가장 영향력이 큰 보안 책임자들은 회사에서 전략적 입장을 피력할 수 있습니다.[3] 이들은 고위 경영진의 일원으로 정보를 수집할 수 있고 경영진과 함께 보안/리스크 위원회를 열 수 있는 권한을 가지며 리스크를 관리하고 적절한 대응책을 마련하기 위한 효과적인 측정 기준을 보유합니다.

IBM의 리스크 관리 팀은 최고 자문 위원회와 분기별로 회의를 엽니다. 이 자문 위원회에는 CEO에게 직접 보고하는 모든 사업부의 수석 부사장들과 함께 재무, 마케팅, 기술 등의 여러 영역을 담당하는 책임자가 포함되어 있습니다. 이들은 각자의 부서에 존재하는 보안 리스크와 보안 통제 수단을 확실히 이해해야 합니다. 회의에서 이 책임자들은 전략을 구성하고 결정합니다. 궁극적으로 보안은 각 부서를 넘어 회사 전체의 미래를 좌우하기 때문입니다.

[3] "Finding a Strategic Voice: Insights from the 2012 IBM Chief Information Security Officer Assessment", IBM Center for Applied Insights, 2012년 5월, http://www.ibm.com/smarter/cai/security

대화에 참여

다른 기사를 보거나, CIO가 염두에 두어야 할 보안의 핵심에 관해 자세히 알아보거나, 다른 보안 리더들과 의견을 나누려면 **ibm.com/smarter/cai/security**를 방문하십시오.

저자 소개

Kristin Lovejoy(klovejoy@us.ibm.com)는 IBM의 CIO 오피스에서 IT 리스크를 담당하는 부사장입니다.

IBM Center for Applied Insights 소개

IBM Center for Applied Insights는 새로운 방식의 사고와 업무, 리더십을 소개합니다. 증거에 입각한 연구 조사를 통해 비즈니스 리더들에게 실용적인 지침과 변혁의 사례를 제공하고 있습니다.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
March 2012

WGW03005-USEN-00