IBM 기업가치연구소

디지털 시대의 위협 관리

최고 임원(C-suite)의 보안, 위험 및 규제 준수 문제 해결

IBM 기업가치연구소

IBM 글로벌 비즈니스 서비스는 IBM 기업가치연구소를 통해 기업 경영진에게 공공 및 민간 부문의 중요한 문제에 관하여 사실에 기초한 전략적 통찰을 제시합니다. 이 임원 보고서는 기업의 비즈니스 가치 실현에 유용한 분석과 의견을 제공하고자 하는 IBM 글로벌 비즈니스 서비스의 지속적 노력의 일환입니다. 자세한 내용이 필요하시면 저자에게 문의하거나 *iibv@us.ibm.com*으로 이메일을 보내주시기 바랍니다. IBM 기업가치연구소의 추가 연구 자료는 *ibm.com/iibv*에서 확인할 수 있습니다.

저자: John Lainhart, Steve Robinson 및 Marc van Zadelhoff

최근 미디어에서 주목하는 문제는 업계를 불문하고 수많은 기업에 영향을 미치는 보안 침해의 확산입니다. 이러한 보안 실패는 피해를 입은 기업에 막대한 비용 지출을 초래할 뿐만 아니라, 고객 신뢰와 브랜드 명성에도 심각한 손상을 야기합니다. 보안은 더 이상 IT 부서의 소관으로 치부할 문제가 아니라 이제 최고 임원(C-suite)의 우선 과제입니다. 기업은 오늘날의 정보 중심 경제에서 보안 위협을 해결하고 규제 준수 요구 사항을 관리하기 위하여 보다 체계적이고 사전 예방적인 대응 방식을 마련해야 합니다.

전 세계가 더욱 디지털화되고 상호 연결됨에 따라 새로운 위협과 문제가 발생할 가능성이 한층 증가했습니다. 현재 상품, 여권, 건물 및 동물을 비롯한 수십억 개 항목에 RFID 태그가 부착되고 있습니다. 2010년 말에는 인터넷 사용자가 20억 명, 휴대 전화 가입자가 50억 명을 넘어섰으며, 이는 전 세계에 인구 3명 가운데 1명이 인터넷을 사용한다는 의미입니다.[1] 2020년에는 자동차, 가전 제품 및 카메라를 비롯하여 500억 개 이상의 항목이 디지털 방식으로 연결될 것으로 예상됩니다.[2] 이와 같이 복잡한 상황에 더하여 전 세계에서 생성되고 복제되는 디지털 정보의 양은 2020년까지 거의 35조 기가바이트에 달할 것으로 전망됩니다.[3]

정보의 양만 증가한 것이 아니라 그에 따른 디지털 자산의 가치도 증가했습니다. 고객 기밀, 지적 자산 및 주요 설비의 제어에 이르기까지 점점 더 많은 정보가 전자적 형태로 사용되는 추세입니다. 이러한 자산에 영향을 미치는 위협은 IT 부서는 물론 조직 전체에 막대한 영향을 줍니다. 예를 들어, Stuxnet 바이러스는 우라늄 정제를 담당하는 프로세스 컨트롤러를 변경하여 고도로 위험한 물질인 우라늄을 안전하게 처리하고 제어하는 기능을 훼손했습니다.[4] 이 사례는 기업의 기술적 인프라를 대상으로 하는 공격 행위가 사회적으로도 영향을 미칠 수 있다는 사실을 극명하게 보여 줍니다.

데이터, 관리 장치 및 소통의 기하 급수적인 증가 외에도 기업이 보안 및 규제 준수를 관리하는 방식을 변경하도록 압박하는 다른 요인들이 있습니다. 기업 내의 유용한 데이터는 경제적 이익과 같은 범죄적 이유, 복수나 불만과 같은 개인적 이유 또는 테러와 같은 정치적 이유 등으로 시스템을 공격하는 자들의 표적이 됩니다. 정보 및 정보 처리 인프라의 피해는 갈수록 빈번하게 그리고 보다 더 체계적이며 "전문적인" 방식으로 발생하고 있습니다.

따라서 중요한 정보 및 관련 자산의 보안이 더욱 중요해지고 어려워졌습니다. 보안의 중요성은 빠르게 증가했으며, 이제는 브랜드의 잠재적 위험을 평가하는 CMO, 보안 사고의 재정적 영향을 파악하는 CFO, IT 시스템의 붕괴가 지속적인 운영에 미치는 영향을 평가하는 COO를 비롯하여 모든 최고 임원이 주목하는 문제가 되었습니다. 보안 인텔리전스(잠재적 위협에 대하여 사전 예방적으로 예측, 파악 및 대응하는 능력)의 개발은 디지털 시대에 새로운 우선 순위를 갖게 되었습니다.

어느 때보다 심각한 보안 문제

데이터, 장치 및 연결이 증가함에 따라 보안 문제의 수와 범위가 지속적으로 증가하고 있습니다. 보안 문제는 외부 위협, 내부 위협 및 규제 준수 요구 사항이라는 세 가지 주요 범주로 분류할 수 있습니다.

외부 위협

최근 대기업 및 정부 기관을 겨냥한 외부 공격이 급증하고 있습니다. 과거에 이러한 위협은 독립적으로 활동하는 개인에 의해 이루어졌으나, 이제는 보다 조직적으로 변모하여 해커 또는 "핵티비스트"로 구성된 집단, 범죄 조직 및 심지어 정부 지원을 받는 조직에 의해 자행되고 있습니다. 공격자들의 동기는 더 이상 이익 추구에 국한하지 않으며, 때로는 명성을 추구하거나 첩보 행위를 목표로 하는 경우도 있습니다. 이러한 공격은 고객 데이터베이스, 지적 자산뿐 아니라 정보 시스템을 통해 운영되는 물리적 자산을 포함하여 그 어느 때보다 중요성이 대두되는 기업의 자산을 목표로 합니다.

이러한 외부 공격은 심각한 재정적 손해를 야기합니다. 예를 들어 Epsilon의 고객 데이터 유출 사고는 수백만 소비자의 이메일 주소를 노출하고 수많은 기업 고객에게 직접적인 영향을 미쳤습니다. 초기의 수습 비용과 장기적인 소송 위험을 합산하면 피해액이 수억 달러에 달할 것으로 추정됩니다.[5] 금융 서비스, 미디어 및 엔터테인먼트, 소매 및 통신 업계의 다른 많은 기업들도 최근 고객의 개인 정보 및 금융 정보에 대하여 유사한 형태의 침해 사고를 보고한 바 있으며, 각 경우에 상당한 IT, 법적 및 규제 준수 비용이 발생했습니다.

내부 위협

정보 보안의 침해는 외부인이 아니라 내부인에 의하여 발생하는 경우가 많습니다. 오늘날 내부인의 범위는 직원, 계약 직원, 컨설턴트는 물론 파트너와 서비스 제공업체까지 포함할 수 있습니다. 보안 침해는 부주의한 행동 및 관리상의 실수(예: 다른 사람에게 암호를 제공하거나, 백업 테이프 또는 랩톱 컴퓨터를 분실하거나, 기밀 정보를 부주의하게 노출하는 경우)에서 불만을 가진 직원의 의도적인 행위에 이르기까지 다양합니다.

이러한 행위는 외부 공격과 마찬가지로 위험합니다. 기밀 기록이 승인 없이 유출된 경우인 위키리크스 사건을 보더라도 미국 정부는 수백만 달러의 손실을 입었으며 전 세계 외국 정부와의 관계도 훼손되었습니다.[6]

규제 준수 요구 사항

기업들은 보안과 관련하여 지속적으로 증가하는 국가, 산업 및 지역의 요구 사항을 준수하라는 요청을 받고 있습니다. 이러한 요구 사항은 각각 고유한 기준과 보고 요구 사항을 명시합니다. 예를 들면 우리나라의 개인정보보호법과 내부회계관리제도(K-SOX), 미국의 SOX(Sarbanes-Oxley), COSO, COBIT, 다양한 ISO/IEC 국제 표준, 미국의 HIPAA/HITECH, EU 개인정보 보호지침(EU Privacy Directive), 인도의 정보 보안 및 개인정보보호 기준(Data Security and Privacy Standards), PCI DSS 및 BASEL II 등이 있습니다. 이와 같은 요구 사항을 준수하려면 문제의 우선 순위를 정하고, 적절한 정책과 통제 수단을 개발하고, 규제 준수 실태를 모니터링하기 위하여 상당한 시간과 노력이 소요되는 경우가 많습니다.

최고 임원(C-Suite)의 우선 순위에 미치는 영향

위협과 규제 준수 요구사항은 최고 임원(C-suite) 개개인이 주요 우선 순위를 처리하는 능력에 지대한 영향을 미칩니다. 기술의 역할이 점점 더 중요해짐에 따라 정보 보안과 관련된 문제는 CIO의 업무 영역을 넘어섰습니다. 2008년부터 13,000명 이상의 최고 임원들을 대상으로 실시한 인터뷰는 최고 경영진에 속한 모든 임원이 보안 문제의 영향을 받는다는 사실을 보여줍니다(그림 1 참조).

최고 임원들은 맡은 역할에 따라 각자 다른 보안 문제에 더 높은 우선 순위를 두어야 하지만, 기업의 입장에서는 오늘날의 보안 위험을 해결하기 위해 응집력 있는 방식으로 행동해야 할 필요가 있습니다. 과거에는 보안 문제의 책임 소재를 보다 분명하게 밝힐 수 있었지만 지금은 문제가 발생하면 잠재적 손실이 여러 곳에서 나타나듯이 보안 책임도 조직의 여러 단위에서 공유됩니다.

예를 들어, 브랜드 강화에 매진하는 CMO(Chief Marketing Officers)는 보안 침해로 인하여 개인 정보가 손실될 경우 고객 신뢰와 브랜드 명성을 상실하는 위험에 처할 수 있습니다. 이러한 문제는 분명히 모든 기업에게 주요한 위험이 될 것이며, 손상된 명성을 회복하기 위하여 모든 최고 임원(C-suite)들이 조치를 취해야 할 것입니다.

최고 경영진이 관리하는 보안 위험의 예는 다음과 같습니다.

- CEO(Chief Executive Officer)는 지적 자산 및 비즈니스에 중요한 데이터가 내부인 또는 외부인에 의해 악용될 수 있는지 확인해야 합니다. 이러한 유형의 침입은 시장 점유율과 명성의 잠재적 손실, 규제 준수를 위한 업무 중지와 관련된 위험 및 형사 입건 가능성이라는 면에서 상당한 영향을 미칠 수 있습니다.

	CEO	CFO/COO	CIO	CHRO	CMO
CxO 우선 순위	• 차별화를 통한 경쟁력 유지	• 규제 준수	• 모바일 장치의 사용 확대	• 전사적인 노동 유연성 실현	• 브랜드 강화
보안 위험	• 지적 자산의 악용 • 업무상 기밀 데이터의 악용	• 규제 준수 요구 사항 충족 실패	• 데이터의 급증 • 안전하지 않은 엔드포인트 및 부적절한 접근	• 기밀 데이터의 유출 • 내부인의 부주의한 행동	• 고객 또는 직원의 개인 정보 도난
잠재적 영향	• 시장 점유율 및 명성의 손실 • 형사 입건	• 감사 실패 • 벌금, 손해 배상 및 형사 입건	• 데이터의 기밀성, 무결성 및/또는 사용 가능성의 손실	• 직원 개인정보 보호정책 위반	• 고객 신뢰 상실 • 브랜드 명성 상실

출처: IBM 기업가치연구소에서 최고 임원(C-level) 연구의 일환으로 13,000명 이상의 임원을 대상으로 실시한 대면 인터뷰

그림 1 : 보안 및 규제 준수 요구사항의 해결은 모든 최고 임원(C-suite)의 우선 과제입니다.

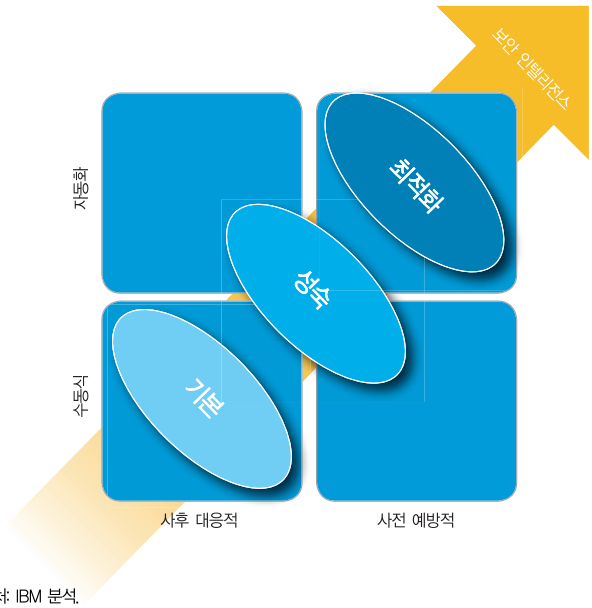
- *CFO(Chief Financial Officer)*는 특히 규제 준수 지침을 충족해야 합니다. 규제 준수 지침의 보안 규정을 준수하지 못하면 감사에 실패하여 기업이 처벌을 받을 뿐 아니라 CFO 본인과 담당 조직이 형사 입건될 수 있습니다.
- *CIO(Chief Information Officer)*는 기업의 유연성 및 유동성을 향상시키기 위하여 데이터 급증, 안전하지 않은 엔드포인트 증가 및 부적절한 데이터 접근과 관련된 문제를 해결해야 합니다. 이러한 문제들은 데이터 기밀성, 무결성 및 가용성의 손실을 초래할 수 있습니다.
- *CHRO(Chief Human Resource Officer)*는 노동력의 유연성을 증가시키기 위하여 직원 개인정보보호정책의 위반을 초래할 수 있는 내부인의 잠재적인 부주의한 행동과 함께 기밀 정보의 유출 가능성을 파악해야 합니다.

요약하면 보안 문제는 더 이상 CIO의 단독 책임이 아니며, CISO(Chief Information Security Officer)에게 위임하는 것만으로 해결되는 문제도 아닙니다. 보안 문제는 모든 최고 임원의 관심과 행동을 필요로 하는 영역입니다.

"보안 인텔리전스" 구현

기업은 위험의 증가 및 그 영향에 대응하기 위하여 보안 문제에 보다 자동화되고 사전 예방적인 대응 방식을 고려해야 합니다. 즉 기업은 비즈니스의 필수 요소로 보안 인텔리전스를 구현해야 합니다. 이를 위해서는 물리적 보안, 데이터 분류, 직원의 경각심 고취 및 통제를 비롯한 다양한 문제에 대하여 종합적인 대응 방식이 필요합니다.

많은 기업에서 보안 인텔리전스는 세 가지 단계를 거쳐 발전합니다. 다시 말하면 위협을 식별, 추적 및 해결하는 데 있어서 수동식 대응 방식에서 점점 더 자동화된 절차를 사용하는 방식으로 변화하고, 보안 문제에 사후 대응적인 방식이 아니라 보다 사전 예방적인 방식을 사용하는 방향으로 변화합니다(그림 2 참조).



출처: IBM 분석.

그림 2 : 보안 인텔리전스를 구현하는 3단계의 체계적 방식

- *기본* – 기업은 물리적 접근과 가상 접근을 모두 통제하는 경계 보호 수단에 집중합니다. 경계 보호는 보안 사고 및 침해에 대한 수동적인 보고를 위한 입력 정보를 제공합니다. 기본 수준의 기업은 방화벽, 바이러스 방지 소프트웨어, 접근 제어 및 수동 보고를 사용하며 이러한 수단은 첫 번째 단계로 유용합니다. 하지만 이 단계의 기업은 실제 보안 상태를 충분히 파악하지 못하고 사후 대응적인 수동식 운영 방식을 사용합니다.

- *성숙* – 보안 분야가 IT 응용 프로그램 및 비즈니스 운영의 구성 요소로 포함됩니다. 이러한 변화에는 주요 응용 프로그램, 데이터베이스 및 비즈니스 절차에 보안을 통합하는 과정이 포함됩니다. 성숙 단계에서는 보안이 보다 종합적으로 다루어지지만 동시에 기업의 보안 작업이 보다 복잡해집니다. 따라서 보안이 보다 널리 확산되지만 긴밀하게 통합되어 관리되는 수준은 약하다는 점에서 기업의 보안 인텔리전스는 여전히 부족한 상태라고 볼 수 있습니다.

- *최적화* – 기업이 보안 인텔리전스 구현을 위하여 예측 가능하고 자동화된 보안 분석을 사용합니다. 과거의 침입, 직원 활동 및 기타 데이터 소스를 프로파일링하여 잠재적 침해가 발생할 수 있는 영역을 미리 파악하고 침해 발생을 사전에 방지함으로써 보안이 최적화 됩니다.

위의 세 가지 단계는 우발적인 보안 사고 및 고의적인 보안 사고에 대하여 모두 추가 대비책을 갖추고 있습니다. 기업의 환경 전반에서 보안 문제를 식별하고 해결하기 위하여, 기업은 분석 능력을 개척하고 활용하여 가장 긴급한 요구사항을 충족해야 합니다. 네 가지 "보안 영역"의 심도 있는 평가는 기업의 통제 방식, 위험 관리 및 규제 준수를 체계적으로 향상시켜 보안 인텔리전스 구현에 기여할 수 있습니다(그림 3 참조).

- *사람* – 암호를 통해 응용 프로그램별로 접근을 제어하는 방식에서 대시보드 및 권한 있는 사용자 제어를 통해 역할별로 사용자 접근을 제어하는 방식으로 전환합니다.
- *데이터* – 기본적인 접근 제어 및 암호화 방식에서 데이터 통제를 개선하고 데이터 사용 및 흐름을 관리하여 데이터를 보호하는 방식으로 이동합니다.
- *응용 프로그램* – 기존 응용 프로그램의 취약점을 조사하는 데 의존하는 방식에서 벗어나 부정 행위를 감지하고 새로운 응용 프로그램에 보안 기능을 포함하는 방식으로 진화합니다.
- *인프라* – 권한 없는 접근과 바이러스를 차단하는 등의 사후 대응적 방식을 고급 네트워크 모니터링 및 진단을 통해 시스템 보안을 유지하는 사전 예방적 방식으로 대체합니다.

보안 영역	오늘날	발전 방향	미래: 보안 인텔리전스	
사람	응용 프로그램별로 ID 관리		역할 기반의 대시보드 및 권한 있는 사용자 관리 구현	고급 상관 관계 및 심도 있는 분석 적용
데이터	접근 제어 및 암호화 구현		사용을 모니터링하고 문제 영역을 관리	
응용 프로그램	취약점 탐지		처음부터 보안을 고려하여 설계	
인프라	원하지 않는 네트워크 접근과 바이러스 차단		고급 위협 감지 및 진단 기능을 실시간으로 실행	

사후 대응적 ⟶ **사전 예방적**

출처: IBM 분석.

그림 3 : 물리적, 기술적 및 인적 자산을 관리하기 위하여 균형 있는 방식이 필요합니다.

최고 임원이 세워야 할 3가지 계획

최고 임원(C-suite)은 보안 인텔리전스를 구현하기 위하여 세 가지 주요 방법을 사용해야 합니다.

- 정보화: 체계적인 방식을 통해 비즈니스 및 IT 위험을 평가합니다.
- 통합화: 광범위한 기업 환경 전반에 우수한 보안 시스템을 구현하고 실행합니다.
- 스마트화: 분석을 통해 위험을 사전 예방적으로 파악하고 위협을 식별, 모니터링 및 해결합니다.

1. 정보화

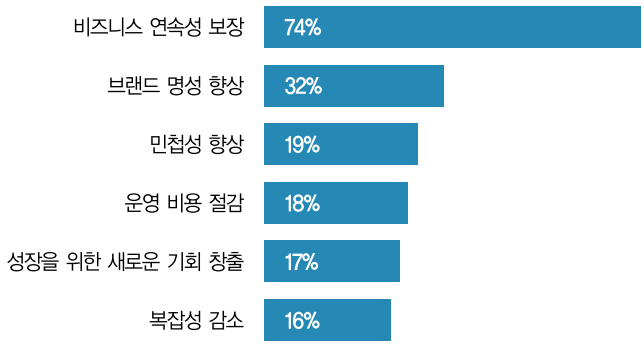
정보화는 보다 광범위한 기업 위험 관리 프레임 워크(그림 4 참조)를 통해 IT 보안 위험을 해결하는 방법입니다.

출처: IBM 기업가치연구소. "2010 IBM 글로벌 IT 위험 연구". 2010년 9월.

그림 4 : 운영 위험 관리를 위한 주요 단계

이 프레임워크는 비즈니스 및 IT 위험을 평가하는 체계적인 방식으로, 여기에는 주요 위협과 규제 준수 요구 사항을 파악하고, 기존의 보안 위험 및 과제를 검토하고, 위험 관리 절차 및 일반 제어 프레임워크를 구현하고, 위기 발생 시 사고 관리 절차를 실행하는 조치가 연관됩니다. 또 다른 중요한 조치는 최고 임원 수준에서 위험 관리 임원(Risk Executive)을 임명하여 정기적으로 이사진과 협업하고, 보안 관련 문제를 조사하고, 업무 중에 IT 위험과 관련한 논의를 활성화하도록 만드는 것입니다.

IBM 글로벌 IT 위험 연구의 설문 응답자들은 IT 위험 관리에 대한 투자가 상당한 비즈니스 이점을 제공한다는 데 동의했으며, 특히 비즈니스 연속성(74%)과 회사의 명성 보호(32%, 그림 5 참조)라는 관점에서 동의한 응답자가 많았습니다. 응답자들에 따르면 IT 위험의 관리는 방어적인 전략 이상의 문제로 간주되어야 합니다. 또한 응답자들은 IT 위험을 보다 효과적으로 관리하여 얻을 수 있는 이점으로 민첩성 향상, 비용 절감, 새로운 성장 기회 창출, 복잡성 감소 등을 들었습니다.[7]



출처: IBM 기업가치연구소. "2010 IBM 글로벌 IT 위험 연구". 2010년 9월.

그림 5 : IT 위험 관리 향상의 이점

사례:

IT 보안 관리 위험과 관련된 감사를 계기로 IT 관리를 쇄신

미국의 대규모 금융 기관이 회사 안팎에서 중대한 IT 관리 및 비즈니스 운영 과제에 직면했습니다. 외부 감사자에 의해 SOX(Sarbanes-Oxley) 결함을 비롯한 여러 가지 중요한 규정의 미준수 사실이 발견되었으며, 내부 감사에서도 여러 건의 불리한 IT 보안 보고서가 작성되었습니다.

이 기업은 업계의 모범 사례를 바탕으로 광범위하고 강력한 통제 프로그램을 마련하는 동시에 새로운 통제 방식이 정기적으로 업데이트 및 개선될 수 있도록 지원하는 시스템을 구축했습니다. 이를 위해 제일 먼저 기업의 보안과 함께 IT 일반 관리, 응용 프로그램 관리, IT 관리를 비롯한 전반적인 관리 시스템을 종합적으로 평가했습니다. 또한 기업의 정보 보안 관리 상태를 평가하는 동시에 보안 절차를 검토하고 정책, 표준 및 절차를 새로 작성하거나 업데이트했습니다.

이를 통해 식별된 문제는 명확한 정책, 표준 및 절차를 갖춘 네 개의 IT 관리 위원회를 수립하여 해결했습니다. 또한 보안, 데이터 무결성, 변화 관리 및 운영 면에서 재무 보고와 관련된 문제 및 취약점을 성공적으로 교정하는 IT 관리 프레임워크와 지원 수단을 구현했습니다.

이러한 노력의 결과로 이 금융 기관은 재무제표 감사를 성공적으로 완료하고 외부 감사 기관으로부터 SOX 평가를 받았습니다. 이는 3년 전에는 불가능한 일이었습니다. 이러한 변화를 통해 이 기업은 SEC (Securities and Exchange Commission)에 신규 일반주를 등록할 수 있었고 그 결과 투자자의 신뢰가 향상되고 주식 가치가 상승하는 성과를 거두었습니다. 또한 IT 관리 라이프사이클 프로그램을 제도화하여 IT 관리와 보안 절차 및 방침을 지속적으로 개선할 수 있게 되었습니다.

2. 통합화

보안은 조직의 경계에 국한된 문제가 아닙니다. 성공적인 기업은 우수한 보안 시스템을 확장된 기업 환경 전반에서 구현하고 실행해야 합니다. 이러한 노력에는 다음과 같은 주요 이해 관계자가 관련됩니다.

- *고객* – 개인정보 보호정책을 개발하고 전달합니다. 투명성을 유지하고 개인정보 보호정책 침해 문제를 신속하게 처리합니다.
- *직원* – 보안 및 개인정보 보호정책과 관련한 요구 사항을 명확하게 규정합니다. 보안 위험을 식별하고 해결하기 위해 필요한 교육을 제공합니다. 시스템 및 데이터의 접근과 사용을 관리합니다.
- *파트너* – 서로 다른 공급망의 조직과 협업하여 보안 기준을 개발하고 구현합니다. 업무 운영을 위한 일상적인 절차로 보안 사고를 포함한 위험을 보고하고 관리합니다.
- *감사자* – 기업 현황과 IT 위험을 평가합니다. 관리 프레임워크를 지원합니다. 외부 규제 준수 정책 및 기업 내부 정책을 정기적으로 검토합니다.
- *조정자* – 규제 준수 위험을 관리하고 기존 규제 사항의 준수를 입증합니다. 변화하는 요구 사항에 따라 기존의 제어 방식을 검토하고 수정합니다.

사례:

효과적인 관리를 통해 기업의 규제 준수를 지원하고 감사 대응 능력을 개선

해마다 수많은 감사를 실시하는 미국의 한 건강 보험 회사는 각 감사 보고서를 사후 대응 방식으로 처리하는 대신 사전에 위험을 관리하고 비용을 절감하는 제어 수단을 마련하여 유지하고자 했습니다. 또한 감사가 업무에 미치는 영향을 줄이고자 했으며, HIPAA(Health Insurance Portability and Accountability Act) 및 NAIC(National Association of Insurance Commissioners) 표준 감사 규정과 같은 새로운 보험업 규제 요구 사항을 준수하기 위한 수단을 확립해야 했습니다.

그 해결책 중 하나는 회사의 IT 프로세스 관리 체계를 정비하는 것이었습니다. 이 회사는 이러한 노력의 일환으로 모든 운영 및 업무 단위에 걸쳐 15가지 주요 IT 프로세스의 관리 방침을 포함하여 업계 표준 IT 관리 조치를 제정했습니다. 각 조치마다 주기적으로 반복되는 프로세스가 사용되었으며, 이러한 프로세스는 관리 절차를 수립, 구현 및 시행하고, 테스트하고, 마지막으로 결과를 모니터링 및 보고하여 위험을 식별하고 관리 프레임워크를 규정했습니다.

새로운 제어 조치는 이 회사가 업계 규정과 표준을 준수하도록 지원하고, 비즈니스 및 IT를 보다 효과적으로 조율하고, 위험을 관리하고 보안을 강화하는 데 기여했습니다. 이 회사는 이제 감사를 보다 효율적이고 일관적인 대응 방식으로 처리할 수 있게 되었으며, 감사 대응에 필요한 노력도 약 절반 수준으로 감소했습니다.

3. 스마트화

위험을 사전 예방적으로 파악하고 위협을 식별, 모니터링 및 해결하는 분석을 사용해야 합니다. 기업에서 보안을 강화해야 함에 따라, 예측 분석의 사용이 더욱 중요해졌습니다(그림 6 참조). 기업은 정교한 상관 관계 분석을 수행하여 고도의 지속적인 위협을 감지하고, 통제력을 보유하고, 보안 인텔리전스 구현을 위하여 중요한 요소인 자동화된 기업 위험 관리 프로세스를 구현할 수 있습니다.

여기에는 다음과 같은 능력이 연관됩니다.

- 이전의 보안 침해 패턴 및 외부 위협을 식별하여 잠재적 공격 영역 예측
- 직원들의 시스템 행동을 조사하여 잠재적인 오용 패턴 식별
- 외부 환경을 모니터링하여 잠재적 보안 위협 식별

보안 인텔리전스

	사람	데이터	응용 프로그램	인프라
최적화	• 통제, 위험 및 규제 준수 • 고급 상관 관계 분석 및 심화 분석			
	• 역할 기반 분석 • 권한 있는 사용자 제어	• 데이터 흐름 분석 • 데이터 통제	• 보안 응용 프로그램 개발 • 부정 행위 감지	• 고급 네트워크 모니터링/진단 • 시스템 보안
숙달	• ID 관리 • 강력한 인증	• 활동 모니터링 • 데이터 손실 방지	• 응용 프로그램 방화벽 • 소스 코드 스캔	• 자산 관리 • 엔드포인트/네트워크 보안 관리
기본	• 암호 및 사용자 ID	• 암호화 • 접근 제어	• 취약점 스캔	• 경계 보안 • 바이러스 방지

출처: IBM 분석.

그림 6 : 분석을 사용하여 사전 예방적으로 위험을 파악하고 위협을 식별, 모니터링 및 해결합니다.

사례:

분석을 통해 보안 위험 대응 능력을 향상

한 글로벌 제약 회사는 위협을 해결하는 보다 "스마트한" 방식을 모색하는 동시에 다양한 공급업체들의 보안 환경을 관리하기 위한 비용과 복잡성을 줄이고자 했습니다. 기존에는 인프라에서는 보고되는 보안 위협과 취약점 데이터 간의 상관 관계가 파악되지 않아 정말로 중요한 사고를 식별하기가 어려웠습니다. 또한 여러 보안 장치를 통해 사전 예방적 활동을 위한 실시간 경고 모니터링이나 보안 침해가 발생하기 전에 조치를 취하기 위하여 숙련된 인적 자원이 필요했습니다.

이 회사는 보안 소프트웨어 솔루션을 사용하고 전문가 및 관리 서비스 업체에 자문을 구하여 보호 범위를 확대하고 비용 및 복잡성을 줄이는 데 성공했습니다. 지금은 회사 전체의 컴퓨팅 환경에서 여러 공급업체의 수백만 개의 보안 이벤트가 분석되고 있으며 정교한 분석을 통해 실시간으로 보안 이벤트 데이터를 처리하고 있습니다. 전문적인 해결 지침을 사용하여 문제를 신속하게 수정하고 취약 영역을 줄이고 있습니다. 또한 보고서를 통해 취약점 및 위협 데이터를 시간의 흐름에 따라 추적하고 관련 동향을 파악하여 보안 상태를 보다 폭넓은 시각으로 파악합니다.

이 회사는 이러한 보안 개혁의 일환으로 다섯 개의 공급업체 환경을 하나로 통합했습니다. 더욱 중요한 점은 사전 예방적인 방식을 채택함으로써 보안 관리 비용이 57% 감소했으며 심각한 보안 이벤트가 하루 10,000건에서 15건으로 대폭 감소했다는 사실입니다.

보안 인텔리전스 구현과 관련된 질문

기업은 잠재적인 위협과, 보다 높은 수준의 보안 인텔리전스를 통해 이러한 위험을 완화할 수 있는 기회를 염두에 두고 다음과 같은 질문에 대한 답을 생각해 보아야 합니다.

여러 보안 영역에 대한 고려

- 보안 위험을 평가하기 위한 계획은 무엇입니까?
- 다양한 영역에서 어떻게 위협을 감지하고 규제 준수를 보고할 수 있습니까?
- 기록 유지 및 감사 능력을 갖추고 있습니까?
- 사건 대응 및 재해 복구를 처리하기 위하여 어떤 프로세스를 사용하고 있습니까?
- 보안 문제에 주요 내부 및 외부 이해관계자를 어떻게 참여시키고 있습니까?

사람

- ID 프로그램을 어느 범위까지 시행하고 있습니까?
- 허가 받은 사용자들이 무엇을 하는지 어떻게 알 수 있습니까?
- ID 및 역할 기반 관리를 자동화하기 위한 계획은 무엇입니까?

데이터

- 기밀 데이터를 분류하고 암호화하는 데 사용하는 방법은 무엇입니까?
- 중요한 데이터가 네트워크 밖으로 유출되는지 어떻게 알 수 있습니까?
- 권한 있는 접근을 포함하여 데이터에 대한 접근을 모니터링하는 방법은 무엇입니까?

응용 프로그램

- 응용 프로그램 개발 프로세스에 어떠한 방법으로 처음부터 보안을 구현하고 있습니까?
- 웹 사이트의 취약점을 정기적으로 테스트하는 방법은 무엇입니까?
- 잠재적 노출에 대하여 기존 응용 프로그램을 테스트하는 방법은 무엇입니까?

인프라

- 연결된 장치들을 신속하게 조정하는 방법은 무엇입니까?
- 발신 네트워크 트래픽과 수신 네트워크 트래픽을 어떤 방법으로 모니터링합니까?
- 새로운 시도(클라우드, 모바일 등)에 보안을 어떻게 구현합니까?

결론: 현실적 위험이 최고 임원들 (C-suite)의 총체적 노력 촉구

오늘날 갈수록 복잡해지고 상호 연관성이 높아지는 세계에서 위험은 실재하며 기하급수적으로 증가하고 있습니다. 보안 문제를 CIO에게만 위임하는 기업은 위험 요소를 키우는 것입니다. 기업에서 유통되는 데이터 및 지적 자산의 보안에 있어 각각의 최고 임원이 담당하는 역할과 비중이 그 어느 때보다 중요해졌습니다(그림 7 참조). 한 가지 공통된 이해 분모는 오늘날 보안이 기술적 문제 이상의 과제라는 사실입니다. 보안은 위험에 대한 숨김없는 논의, 투자 그리고 보안 문제에 대한 사전 예방적 대응을 필요로 합니다.

잠재적인 위험과 우발적인 사고의 모든 경우를 비용 효율적으로 해결할 수는 없습니다. 기업은 생각할 수 있는 모든 위협에 대하여 보호 조치를 취하려고 노력하기보다는 잠재적 위험의 비즈니스 영향에 우선 순위를 매겨야 합니다. 이와 같은 우선 순위 평가는 각자 특정 분야에 대하여 고유한 관점을 제공하는 여러 최고 임원(C-suite)들의 의견을 토대로 이루어집니다.

IBM 기업가치연구소의 본 연구에 대한 자세한 내용은 iibv@us.ibm.com으로 문의하십시오. IBM 기업가치연구소의 연구에 대한 전체 카탈로그는 다음 웹 사이트에서 확인할 수 있습니다.
ibm.com/iibv

IBM 기업가치연구소의 최신 연구 결과를 가장 먼저 받아 보십시오. 아래 주소에서 IdeaWatch를 구독하시기 바랍니다. IdeaWatch는 IBM 기업가치연구소의 연구를 토대로 전략적 통찰과 권장 사항을 제공하는 임원 보고서가 포함된 월간 전자 뉴스레터입니다.
ibm.com/gbs/ideawatch/subscribe

CEO	CFO	COO	CIO	CHRO	CMO
보안 위험이 주주 가치 및 신뢰에 영향을 미치지 않도록 예방	유해한 보안 이벤트의 재무적 영향 파악	IT 시스템 중단이 진행 중인 운영 사업에 미치는 영향 평가	비즈니스 전반에 정보 보안의 실패가 야기하는 부작용 이해	직원 데이터의 부당한 유출과 관련된 위험 해결	보안 침해와 관련된 브랜드 문제 해결

출처: IBM 분석.

그림 7 : 보안은 최고 임원(C-suite)의 책임입니다.

변화하는 세계에서의 든든한 파트너

IBM은 고객과 협력하여 비즈니스 통찰력, 고급 연구 및 기술을 종합하여 오늘날과 같이 빠르게 변화하는 환경에서 확실한 이점을 제공합니다. 비즈니스 설계 및 실행에 대한 IBM의 통합된 방식을 통해 전략을 행동으로 실현할 수 있도록 도와 드립니다. 또한 IBM은 17개 업종의 전문 기술과 170개국에 걸친 세계적인 네트워크를 사용하여 고객이 전 세계에서 변화를 선도하고 새로운 기회에서 수익을 창출할 수 있도록 지원합니다.

저자 정보

John Lainhart는 IBM 글로벌 비즈니스 서비스의 글로벌 보안 및 개인정보보호 서비스 영역 리더이자 미국 공공 부문 사이버보안 및 개인정보보호 서비스 영역 리더입니다. 그는 AICPA(American Institute of Certified Public Accountant)의 인증서비스집행위원회(Assurance Services Executive Committee)에 속한 데이터 무결성 태스크포스(Data Integrity Task Force) 및 인터넷보안센터 전략자문위원회(Strategic Advisory Council for the Center for Internet Security)에서 IBM을 대표하고 있습니다. 또한 정보시스템감사 통제협회(Information Systems Audit and Control Association)와 정보기술관리협회(IT Governance Institute)에서 국제 회장을 비롯하여 여러 직위를 역임했으며, 현재 기획 위원회(Framework Committee)의 일원이자 CobiT® 5 태스크포스의 공동 회장이며 IT 운영, CobiT®, ValIT® 및 RiskIT® 관련 이니셔티브의 주요 자원봉사 고문을 맡고 있습니다. 연락처는 *john.w.lainhart@us.ibm.com*입니다.

Steve Robinson은 IBM 보안 솔루션을 총괄하는 사장으로서 다양한 보안 제품 및 서비스 지역에 걸쳐 IBM 보안 이니셔티브의 전 세계적인 책임을 맡고 있습니다. 그는 전략 리더로서 마케팅 및 보안 영업 팀은 물론 소프트웨어, 하드웨어 및 서비스 부문의 개발 팀에 이르기까지 지침을 제공하고 있습니다. 이 역할을 담당하기 전에는 2005년부터 IBM Rational Software의 글로벌 영업 부문 부회장으로서 1,000명 이상의 영업 전문가, 채널 팀은 물론 비즈니스 파트너, 시스템 통합 업체 및 ISV로 구성된 광범위한 커뮤니티를 이끌며 Rational 브랜드의 영업 전략 및 업무 수행을 담당했습니다. 그는 1984년에 IBM에 입사하여 영업, 기술 서비스 및 제품 관리 부문에서 수많은 임원직 및 관리직을 역임했습니다. 연락처는 *steve_robinson@us.ibm.com*입니다.

Marc van Zadelhoff는 IBM 보안 솔루션의 글로벌 전략 이사로서 전 세계적으로 IBM의 소프트웨어 및 서비스 포트폴리오를 위한 전반적인 오퍼링 관리, 예산 및 포지셔닝을 담당합니다. 그는 이러한 업무의 일환으로 IBM의 고객 자문 위원회를 운영하면서 IBM의 방향을 개척하기 위하여 전 세계의 고객들을 만나고 있습니다. 이전에는 IBM에서 Tivoli의 보안 M&A와 인수된 ISS(Internet Security Systems) 부문을 위한 마케팅 팀을 운영했으며 가장 최근에는 글로벌 기술 서비스 사업부에서 IBM 보안 서비스를 위한 전략, 포트폴리오 및 비즈니스 개발을 담당했습니다. 그는 전략 컨설턴트로서 경력을 시작했습니다. 연락처는 *marc.vanzadelhoff@us.ibm.com*입니다.

기여자

Linda Ban, Global CIO Study Director, AIS Studies, IBM Institute for Business Value, IBM Global Business Services

Hans A.T. Dekkers, Associate Partner, IBM Global Business Services

Peter Korsten, Partner and Vice President, Global Leader, IBM Institute for Business Value, IBM Global Business Services

Eric Lesser, Research Director and North American Leader, IBM Institute for Business Value, IBM Global Business Services

Kristin Lovejoy, Vice President, IT Risk, IBM BT/CIO organization

Wolfram Stein, Partner and Vice President, Global Strategy & Transformation Service Line Leader Executive, Consulting Services, IBM Global Business Services

Nichola Tiesenga, Partner, Public Sector, Cybersecurity and Privacy, IBM Global Business Services

Marisa Viveros, Vice President, IBM Security Services, IBM Global Technology Services

참조 서적

1 International Telecommunications Union. "Global Number of Internet Users, total and per 100 Inhabitants, 2000–2010." United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls

2 Ericsson. "More than 50 billion connected devices – taking connected devices to mass market and profitability." February 14, 2011.http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c

3 IDC "Digital Universe Study," sponsored by EMC. May 2010.

4 McMillan, Robert. "Siemens: Stuxnet worm hit industrial systems." ComputerWorld. September 14, 2010. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

5 Greene, Tim. "Worst-case projected cost of Epsilon breach: $4B." NetworkWorld. May 1, 2011. http://www.network-world.com/news/ 2011/050111-epsilon-breach-costs.html

6 Fildes, Jonathan. "What is Wikileaks?" BBC. December 7, 2010. http://www.bbc.co.uk/news /technology-10757263

7 Ban, Linda B., Richard Cocchiara, Kristin Lovejoy, RicTelford and Mark Ernest. "The evolving role of IT managers and CIOs." IBM Institute for Business Value. September 2010. http://www 935.ibm.com/services/us/gbs/thoughtleadership/ibv-global-it-risk-study.html

한국IBM Global Business Services
(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩

TEL: (02)3781-7800
www.**ibm.com**/kr

2011년 10월

Printed in Korea

GBE03423-USEN-01