IBM Center for Applied Insights

전략적 발언권 확보

2012년 IBM CISO(Chief Information Security Officer) 평가에서 통찰력 향상

IBM

연구 정보

전 세계 보안 리더의 전략과 접근법을 파악하기 위해 IBM Center for Applied Insights는 기업의 정보 보안을 책임지는 IT 및 비즈니스 라인 경영진 등 138명의 보안 리더와 이중 블라인드 인터뷰를 실시했습니다. 직위가 CISO(Chief Information Security Officer)인 리더들도 있지만 조직 구조의 다양성을 고려할 때 대부분은 그렇지 못했습니다. 또한 25명의 정보 보안 리더들과 심층 대화를 가져 양적 연구의 부족한 점을 보완했습니다.

7개 국가의 광범위한 산업 분야에서 참여하였으며, 응답자의 20%는 직원 수 10,000명 이상인 기업에서, 55%는 직원 수 1,000 ~ 9,999명 기업에서 정보 보안을 이끌고 있습니다.

이 연구와 CIO 및 CISO 대상의 다른 보안 및 리스크 관리 자료를 **ibm.com/smarter/cai/security**에서 이용할 수 있습니다.

상호 연결과 협업이 급증하면서 정보 보안은 갈수록 복잡해지고 관리하기가 어려워졌습니다. 한편 이러한 시대 변화에도 효율적으로 대처해 나가는 보안 조직이 있습니다. 본 연구에서는 이러한 시대적 변화에 따른 보안 조직의 뚜렷한 진행 패턴과 정보 보안에서 우수성과 신뢰성을 보여준 기업들만의 특징을 설명합니다.

이처럼 시대를 앞서 가는 사람들은 보다 능동적이고 통합된 전략적 접근법으로 보안을 실행하며, 에뮬레이션 가치가 있는 모델 및 CISO(Chief Information Security Officer)의 비즈니스 리더십 역할을 중요하게 생각합니다.

오늘날과 같이 고도로 연결된 세상에서 정보 보안은 기술 분야에 국한되지 않고 전사적인 최우선 전략으로 부상했습니다. 뉴스 헤드라인을 잠깐 살펴보는 것만으로도 그 이유를 알 수 있습니다. 2011년에 기업들은 2004년[1] 이후 두 번째 규모의 데이터 손실을 겪었습니다.

보안 리더들은 급격한 변화의 시기 한 가운데에 있습니다. IT가 더 이상 백오피스 또는 기업에 한정되지 않고, 공급자에서 고객에 이르는 전체 가치망이 전자식으로 연결되어 유례없는 협업이 이루어집니다. 다양한 정보 액세스 기기 및 방식이 확산 중이고, 모바일 작업자 수가 2015년에 13억에 다다를 것으로 예상됩니다. 이와 동시에 모바일 보안 위협 요소도 2011년[2]에 최대 20% 증가했습니다. 이처럼 모든 변화로 그 어느 때보다 큰 취약성에 노출되어 있습니다.

대부분의 조직은 위기 대응 단계에 있지만 대응적인 모습에서 벗어나 미래 리스크를 줄이는 능동적인 조치를 취하는 조직도 있습니다. 그들은 스스로 보안 관련 역량이 성숙한 수준이고 새로운 위협 요소를 해결할 만반의 준비를 갖추었다고 판단합니다. 신뢰를 높이기 위해 이 기업들은 어떤 조치를 취했을까요? 더 중요한 점은 이들이 실행한 조치들이 다른 기업들에게 나아갈 방향을 제시하고 있을까요?

"보안 리더들은 정보 기술에 국한되지 않고 보다 독립적으로 비즈니스에 밀접히 통합되고 있습니다."

– IT 수석 부사장, 에너지 및 유틸리티[3]

변화하는 보안 환경: 우리가 알게 된 사실

기업의 가장 중요한 자산인 돈, 고객 데이터, 지적 재산, 브랜드의 보호를 책임지는 보안 리더들은 극심한 압박 하에 있습니다. 본 연구 결과는 이러한 태도의 근본적인 변화와 명백히 인식되는 정보 보안의 전략적 중요성을 밝힙니다.

- **보안 문제에 대한 비즈니스 리더의 우려 증가.** 보안 리더 중 2/3는 2년 전에 비해 오늘날 고위 경영진의 보안에 대한 관심이 커졌는데 주된 이유는 언론의 집중 보도 때문이라고 말합니다.
- **예산 증가 기대.** 보안 리더 중 2/3는 정보 보안 관련 지출이 향후 2년 동안 급증할 것으로 기대합니다. 거의 90%는 2자릿수 증가를 예상하고, 10명 중 1명은 50% 이상의 증가를 예상합니다.
- **리스크 관리에 주력.** 보안 리더들은 2년 안에 미래 리스크를 최소화하는 데 더 많은 시간을 할애하고, 규제 및 규정 준수 문제를 관리하며, 현재 위협 요소를 완화하는 데 할애하는 시간을 절감할 것으로 예상합니다.

- **외부 위협 요소가 주요 보안 과제로.** 내부 위협 요소, 기술 도입 또는 규정 준수보다 외부 위협 요소에 관심이 집중되어 최우선 보안 문제로 대두됩니다.
- **모바일 보안 주력.** 모바일 근무 형태의 증가와 폭발적인 무선 기기 이용으로 보안 리더의 절반 이상은 모바일 보안이 향후 2년 간 제1의 기술 과제가 될 것이라 말합니다.

산업 전반에 걸쳐 정보 보안의 중요성에 대해서는 이견이 없습니다. 대부분의 기업이 중앙 집중적인 보안 기능 구현을 보고하고 있지만, 그들의 조치와 계획, 전략을 면밀히 살펴본 후 각 조직들이 "중앙 집중식" 보안을 실제로 구현하는 방식에는 커다란 차이가 있음을 알게 되었습니다.

성숙도 및 준비성 자체 평가

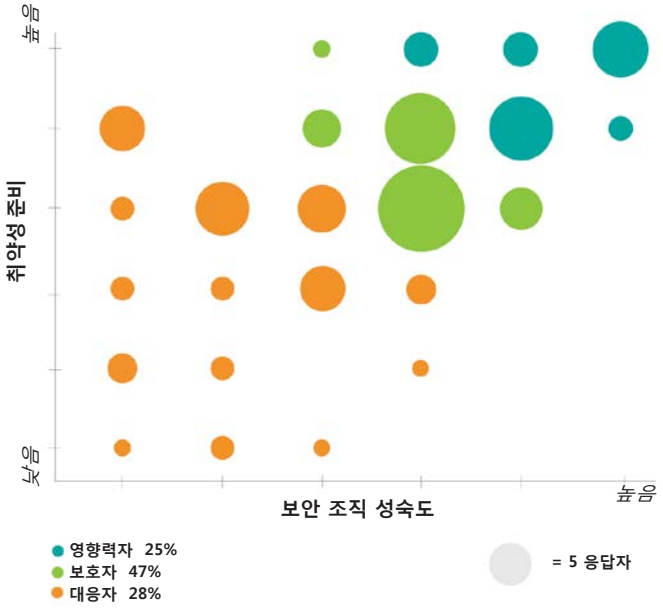

그림 1: 보안 리더의 1/4만이 조직이 성숙한 단계이고, 취약점을 예방하거나 방지하는 능력을 자신 있게 구축했다고 생각합니다.

"보안 리더들의 비즈니스 책임이 커지고 그 대상이 점점 확대되고 있습니다."

– CIO, 보험

조직의 준비 상태

조직이 보안 취약점을 처리하거나 예방하는 능력 및 그 성숙도를 자체 평가 시 조직을 다음 3가지 유형으로 나눌 수 있습니다(그림 1 참조).

- **영향력자** – 설문 조사 대상자의 25%를 차지하는 이 그룹은 자사의 보안 조직을 성숙도와 준비성 면에서 매우 높게 평가하며 혁신적이라고 생각합니다. 이 보안 리더들은 기업에서 비즈니스 영향력과 권한을 가진 전략적 발언권자입니다.
- **보호자** – IBM 조사 대상의 절반을 차지하는 이 보안 리더들은 정보 보안의 중요성을 전략적 우선 과제로 인식하지만, 기업의 보안 접근법을 개혁하는 데 중요한 측정 통찰력과 필요한 예산 권한이 부족합니다.
- **대응자** – 이 그룹은 대부분 대응 단계에 머물며 기업을 보호하고 규정 및 표준을 준수하기 위해 노력하지만, 전략적으로 진전을 이루는 데 어려움을 느낍니다. 아직 중요한 변화를 이끌 자원이나 비즈니스 영향력은 가지고 있지 않습니다.

확신과 자신감을 가진 기업과 격차를 보이는 기업의 모습은 중요한 질문을 제기합니다. 영향력자의 어떤 차이가 이러한 결과를 유발할까요?

영향력자 그룹의 특징

흥미롭게도, 이 3가지 보안 분류가 특정 인구 통계에 편향되지 않고 모든 그룹에서 산업, 지역, 기업 규모가 고르게 혼합되어 분포합니다. 주요 차이점은 구조, 범위, 책임성 등 정보 보안 프로파일에 있습니다. 보안 리더의 응답을 분석한 후 보안 조직의 뚜렷한 진행 패턴(그림 2 참조)과 가장 우수한 조직의 특징을 알게 되었습니다.

"정보 보안 리더의 발언권이 커질수록 기업 내 영향력과 의사 결정 파워가 커질 것입니다."

– IT 사업부 책임자, 미디어 및 엔터테인먼트

보안 프로파일

		대응자	보호자	영향력자
구조 및 관리	전담 CISO	26%	42%	56%
	보안/리스크	26%	52%	68%
	위원회 예산 라인	27%	45%	71%
	예산 권한	CIO (30%) IT VP/책임자/관리자 (24%) CFO (18%)	CIO (32%) CFO (20%) CEO (20%)	CIO (26%) CEO (26%) CISO (13%)
조직 범위	리더십 관심 증가	50%	68%	77%
	정기적인 이사회 주제	22%	58%	60%
	향후 2년 간 주력 분야	새로운 보안 기술 (46%) 비즈니스 프로세스 이해 (36%)	직원 교육 (53%) 새로운 보안 기술 (42%)	직원 교육 (59%) 커뮤니케이션/협업 (24%)
측정	표준화된 지표	26%	43%	59%

그림 2: 영향력자는 정보 보안을 전략적 우선 과제로 격상시킬 가능성이 높습니다.

구조 및 관리

고위 경영진이 접근법 조율의 필요성을 인식하면서 영향력자 그룹에 속한 조직은 전사적 전략 범위의 전담 리더인 CISO를 임명할 가능성이 높습니다. 또한 영향력자는 고위 경영진이 이끄는 보안 총괄 위원회(대개 CISO)를 구축하는 사례가 많습니다. 이 위원회의 주요 목표는 보안 문제를 전체적으로 평가하고 통합된 기업 전략을 개발하는 것입니다. 법적, 비즈니스 운영, 재무, 인적 자원 등 다양한 측면에서 체계적인 변화를 책임집니다.

영향력자 대부분이 그들의 활동을 지원하는 전담 보안 예산 라인을 이용하는데 조사 대상 전체에서는 CIO가 정보 보안 예산을 제어하는 경우가 많았습니다. 그러나, 보호자와 영향력자 조직에서도 투자 권한은 대부분 비즈니스 리더에게 부여됩니다. 사실, 정보 보안 예산을 총괄하는 면에서 CEO와 CIO가 별 차이가 없다는 게 영향력자의 의견입니다.

대응자 조직에서는 CISO와 총괄 위원회가 있는 경우가 드물며, 보안에 대해서는 보다 전술적이며 단편적인 접근법을 제안합니다. 전담 예산 라인이 부족하므로 이니셔티브 범위를 특정 기능이나 사일로로 제한하거나, 자금에 맞춰 기능을 협상해야 하는 순간이 끊임없이 발생합니다.

CISO 관점: 광범위한 시야, 폭넓은 역할

Paul Connelly

부사장 겸 CISO(Chief Information Security Officer), Hospital Corporation of America

몇 가지 주요 동적 변화로 인해 보안 리더 역할이 변하고 있습니다. 대다수 회사들의 경우, 정보의 가치와 볼륨은 증가하고, 정보 위협 요소는 한층 정교하고 무분별해지며, 취약한 보안이 초래하는 희생과 비용은 갈수록 커지고 있습니다. 또한 비즈니스 리더와 고객, 대중의 정보 보호 기대치는 그 어느 때보다 높습니다.

따라서 보안 리더는 회사 데이터를 보호할 수 있는 효율적이며 혁신적인 방법에 주력하고, 단순한 보안 조치에서 벗어나 보다 폭넓은 시각으로 정보 보호를 이해해야 합니다. 정보 보호의 우선 순위와 지출 규모를 비즈니스 수준에서 결정해야 하며, 이는 기존의 IT 보고 구조에 커다란 변화를 가져올 수 있습니다. 리스크 관리, 개인정보보호 정책, 재해 복구, 비즈니스 연속성 계획과 물리적 보안을 조율하여 가시적인 효과를 실현합니다. 중복을 없애고 시너지를 창출하는 동시에 정보 보호 효율성을 높임으로써 보안 리더가 광범위한 범위의 정보 리스크 관리 책임자로 발전할 수 있습니다.

조직 범위

영향력자는 비즈니스 리더와 이사회의 관심을 집중시킬 수 있습니다. 보안은 단기적인 주제가 아닌 비즈니스 회의에서 정기적으로 등장해야 하는 의제이자 문화입니다. 영향력자 보안 리더는 폭넓은 리스크 인식의 필요성을 느끼고 전사적 교육, 협업 및 커뮤니케이션에 주력합니다(그림 3 참조). 또한 기업 보안에서 직원이 보다 능동적인 역할을 하는 문화를 구축하기 위해 비즈니스 경영진과 협력합니다. 비즈니스와 밀접히 통합되어 있으므로 신제품 및 서비스 설계에 영향을 미치고 프로세스 초기에 보안상의 문제를 고려하도록 조성합니다.

향후 2년 간 주력 분야의 차이

대응자		영향력자
	전사적 커뮤니케이션 및 협업 향상	**4x** *증가*
	교육 제공 및 인식 증가	**2x** *증가*
2x *증가*	신기술 통합으로 현재 취약점 보완	

그림 3: 기본적인 보안 기술 및 방식을 구현하면서 영향력자는 관심을 사람에게 돌리고, 리스크 인식 문화를 구축하려고 합니다.

대응자는 전술적으로 접근합니다. 새로운 보안 기술을 통합하여 보안 취약점을 보완하고, 비즈니스 프로세스를 재설계하며, 신규 직원을 고용하는 등 기본 요소에 집중합니다. 영향력자에게 기술 및 비즈니스 프로세스가 여전히 중요한 반면, 대응자는 기본 기능을 구축하는 대신 지속적으로 혁신하고 개선하는 방식을 선호합니다.

3개 그룹 전체에서 모바일 보안은 최우선 기술 과제이면서 응답자(60%)와 보호자(63%)의 중심 의제입니다. 그러나, 영향력자에게는 모바일 보안이 완벽한 전략의 부분입니다. 영향력자는 모바일 액세스 보호(33%)뿐만 아니라, 클라우드 보호(30%) 및 데이터베이스 스토리지 보호(30%)에도 주력합니다.

"보안 리더가 조직의 핵심으로 부상하면서 예산이 증가하고 주변부에서 핵심 역할로 바뀝니다."

– 비즈니스 라인 책임자, 은행

측정

영향력자는 대응자에 비해 진행 상황을 2배 이상 추적하는 경향이 있습니다. 리스크 인식 문화를 구축하고자 하는 의도를 고려할 때 영향력자 조직은 보호자와 대응자에 비해 사용자 인식 및 교육 프로그램에 대한 측정을 보다 중요시합니다 (그림 4 참조). 보다 체계적이고 광범위한 리스크를 우려하므로 미래 위협 요소 및 신기술 통합을 처리하는 능력을 평가할 가능성도 높습니다. 대체적으로, 영향력자는 비즈니스 리더의 관심을 이끌고, 기업 간 협업을 촉진할 뿐만 아니라, 공식 조치를 통해 맡은 업무를 철저히 책임집니다.

"일반적으로 정보 보안의 역할이 특정 리스크에서 벗어나 글로벌 리스크를 대상으로 합니다. 과거보다 그 역할이 대폭 확대되고 있습니다."

– 재무 책임자, 보험

지표의 중요성

그림 4. 영향력자는 다양한 지표를 통해 진행 상태를 측정하여 다른 그룹들보다 체계적 변화에 더 많은 관심을 기울일 수 있습니다.

CISO 관점: 측정이 중요한 이유

John Meakin

보안 솔루션 및 아키텍처 글로벌 책임자, Deutsche Bank

보안 과제의 동적 특성을 고려할 때 조직의 보안 상태를 측정하는 작업의 중요성이 커지고 있습니다. 위협 요소는 항상 변화하며, 솔루션은 단편적이고 동적이면서 점점 복잡해지므로 현재 상태를 파악하는 것이 필수입니다. 주요 지표로, 활성화 이전 특정 보안 요구사항을 정의하고 테스트한 애플리케이션의 수, 알려진 취약점을 수정한 속도, 완벽성 등 다양한 측정 수단이 있습니다.

사람들이 매우 다양한 위치와 기기에서 정보에 액세스하므로 보안이 더욱 어려운 문제가 되었습니다. 정보를 분류하여 저장한 서버 및 엔드포인트를 추적해야 합니다.

각종 수치가 정의하고 캡처해야 하는 과제가 되더라도 조직의 구현을 방해하는 장벽이 되지 않아야 합니다. 처음에는 측정의 정확도가 떨어지지만 시간이 지날수록 향상되며, 이러한 프로세스 자체는 이를 가치 있는 통찰력으로 전환합니다.

보안 리더십 사례

지속적인 위협 요소와 리스크 범위가 늘어남에도 불구하고, 일부 조직은 이를 해결할 수 있는 자신감과 능력을 가지고 있습니다. 이들의 접근법은 폭넓은 보안 기능의 중요성과 정보 보안 리더의 전략적 역할을 강조합니다. 그러나 보다 전체론적 전략을 도입하기 위해서는 획기적인 변화가 동반됩니다.

보안 리더는 비즈니스 리더십 위상을 확보해야 하며, 정보 보안이 기술 지원의 일종이라는 생각을 타파해야 합니다. 정보 보안의 범위는 보안 기술과 프로세스뿐만 아니라, 교육 및 문화의 변화를 포괄합니다. 리더들은 위험 대응과 규정 준수를 넘어 능동적으로 리스크를 관리하는 보안 조직으로 거듭나야 합니다. 정보 보안 관리가 단편적인 개별 이니셔티브에서 통합되고, 체계적인 접근법으로 전환되어야 합니다. 그리고 단편이 아닌 기업 전체를 보호하도록 보안을 설계해야 합니다.

이러한 목표를 실현하기 위해 보안 리더는 현재 능력과 당면 요구사항을 기반으로 실천 계획을 구성해야 합니다. 또한 전사적 변화를 이끌기 위해 전체 C 레벨 임원의 지원을 확보해야 합니다.

대응자는 단순한 전술적 포커스에서 더 발전하기 위해 다음을 수행합니다.

- 전담 보안 리더십 역할(CISO 등)을 구축하고, 보안 및 리스크 위원회를 구성하며, 진행 상황을 측정합니다.
- 보안 혁신에 더 많은 시간과 자원을 할애하여 일상적인 보안 프로세스를 자동화합니다.

보호자는 보안을 보다 전략적인 우선 과제로 만들기 위해 다음을 수행합니다.

- 향후 리스크를 최소화하는데 필요한 예산을 늘립니다.
- 폭넓은 기업 우선순위와 정보 보안 이니셔티브를 조율합니다.
- 보안 동료 네트워크와 협업하고, 노하우를 배웁니다.

영향력자는 보안 접근법을 지속적으로 혁신하고 개선하기 위해 다음을 수행합니다.

- 리스크 인식 문화를 조장하기 위해 커뮤니케이션, 교육 및 비즈니스 리더십 스킬을 더욱 강화합니다.
- 지표 및 데이터 분석으로 얻은 통찰력을 이용하여 가치 높은 개선 영역을 파악합니다.

영향력자의 통합된 접근법, 전략적 범위, 측정 시스템은 신개념의 보안 조직과 지금까지 볼 수 없었던 리더의 모습을 보여줍니다. 이 시대를 앞서가는 보안 리더는 권한, 책임, 영향력을 가지고 있으므로 지속적인 진전을 이룰 수 있습니다. 이러한 리더들의 우수 사례를 바탕으로 지금까지 실현하지 못한 리더들도 전략적인 발언권을 가질 수 있습니다.

자세한 내용

IBM 보안 리더의 관점을 비롯한 추가 통찰력에 대한 자세한 내용은 IBM Center for Applied Insights 정보 보안 웹 사이트 (**ibm.com**/smarter/cai/security)에서 확인하실 수 있습니다. 또한 IBM Institute for Advanced Security (institutefor advancedsecurity.com)의 일부로 전 세계의 동료와 협업할 수 있습니다.

저자 소개

David Jarvis는 IBM Center for Applied Insights의 수석 컨설턴트로, 신흥 비즈니스 및 기술 주제에 대한 사실 기반 연구 전문가입니다. David는 연구 업무 외에도 비즈니스 예측과 창의적인 문제 해결에 대한 강의도 제공합니다. 궁금하신 사항은 djarvis@us.ibm.com으로 문의해 주시기 바랍니다.

*Marc van Zadelhoff*는 Strategy for IBM Security Systems 부사장입니다. 현재 Marc는 IBM의 글로벌 보안 소프트웨어 및 서비스 포트폴리오의 전반적인 오퍼링 관리, 예산, 포지셔닝을 담당하고 있습니다. 궁금하신 사항은 marc.vanzadelhoff@us.ibm.com으로 문의해 주시기 바랍니다.

*Jack Danahy*는 IBM Security Systems 책임자입니다. Jack은 컴퓨터 네트워크 및 데이터 보안 분야의 유명 연설가이자 저자이며, Ponemon Institute의 우수 연구원입니다. 또한 데이터 개인정보 보호정책, 사이버 보안, 사이버 위협 요소, 중요한 인프라 보호 영역에서 산업 및 정부 보안 그룹에 자주 등장하는 기여자이기도 합니다. 궁금하신 사항은 jack.danahy@us.ibm.com으로 문의해 주시기 바랍니다.

IBM 기고자

IBM Center for Applied Insights
Angie Casey, Steve Rogers, Kevin Thompson

IBM Market Development & Insights
Subrata Chatterjee, Doron Shiloach, Jill Wynn

Office of the IBM CIO
Sandy Hawke, Kris Lovejoy

IBM Security Systems
Tim Appleby, Tom Turner

IBM Center for Applied Insights 정보

IBM Center for Applied Insights(ibm.com/smarter/cai/value)에서는 사고, 업무, 리더십에 대한 새로운 방식의 접근법을 도입하고 있습니다. 실제 사례를 바탕으로 이루어진 연구를 통해 리더들에게 실질적인 가이드와 함께 변화를 위한 다양한 사례들을 제공합니다.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2012

1 *Verizon 2012 Data Breach Investigations Report.* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

2 "Mobile Worker Population to Reach 1.3 Billion by 2015, According to IDC." January 2012. http://www.idc.com/getdoc. jsp?containerId =prUS23251912

3 All industry quotes derived from IBM Center for Applied Insights research.

CIE03117-USEN-00