IBM **Center for Applied Insights**

보안 책임자를 위한 새로운 기준

IBM의 '2013 최고 정보 보안 책임자 평가'로부터 얻은 통찰력

지금의 보안으로 충분한가? 적절한 과제에 집중하고 있는가? 다른 조직과 비교했을 때 어느 정도의 수준인가? 최고 정보 보안 책임자(CISO)를 비롯한 보안 책임자들은 이러한 질문을 끊임없이 하고 있을 것입니다. 본 연구에서는 이 질문들에 대한 답을 얻을 수 있도록 비즈니스, 기술 및 평가와 관련된 우수 사례를 소개하며 다양한 과제들도 함께 다뤄볼 것입니다. 보안을 확실하게 구축한 보안 책임자들도 다양한 비즈니스 관련 문제를 관리하고, 모바일 보안 정책을 수립하고, 비즈니스 지표, 리스크 지표 및 보안 지표를 완전히 통합하기 위해 지속적으로 노력하고 있습니다. 보안 방식을 적절히 결합하고 핵심 과제를 해결하는 보안 책임자들은 더욱 다양한 측면에서 성과를 올리면서 새로운 기준을 수립하고 있습니다.

본 연구에 대한 소개

IBM의 2012년도 CISO 평가인 "**Finding a Strategic Voice**"를 더 확대하여 진행하기 위한 목적으로, IBM Center for Applied Insights는 IBM Security Systems 및 IBM Security Services와의 협업을 통해 각 조직에서 정보 보안을 책임지고 있는 고위급 책임자 41명과 심층 인터뷰를 실시했습니다. 인터뷰의 목적은 각 조직에서 실시하고 있는 구체적인 업무 방식과 행동을 확인하여 다른 보안 책임자의 역할과 영향력을 강화하는 것이었습니다.

연속성을 유지하기 위해, 2012년도 연구의 참가자 중 더욱 성숙한 보안 책임자를 중심으로 인터뷰 대상을 모집했으며, 그 결과 본 연구의 인터뷰 대상자의 80%는 이전의 인터뷰 대상자 중에서 선정되었습니다. 인터뷰 대상은 4개국의 광범위한 산업 분야에서 선정되었습니다. 인터뷰 대상의 80% 이상은 대기업과 관련되어 있었으며, 약 3분의 1은 미화 백만 달러 이상의 보안 예산을 가지고 있었습니다.

2012년도 CISO 평가에서 설명한 것과 같이, 전체적인 보안 환경은 여전히 까다롭습니다. 정교한 위협과 모바일 관련 기대치의 증가는 매우 중요한 과제이며, 이로 인해 고위급 경영진들은 보안 책임자에 많은 관심을 두게 되었습니다. 한편, 보안 책임자들은 조직에서 영향력을 얻기 위해 더욱 많은 노력을 들이고 있습니다.[1] 조직은 보안 책임자가 성장하여 정보 리스크 전문가가 되어 주기를 바라고 있습니다.[2] CISO에 대한 관심이 증가하고, CISO에게 단순히 기업을 보호하는 것 이상의 역할이 더 많이 요구됨에 따라 조직의 책임자는 여러 가지 핵심적인 질문에 직면하게 되었습니다. "우리 조직은 적절한 인력과 역량을 보유하고 있는가?", "동종 업계의 다른 보안 책임자와 비교하면 우리 조직은 어떠한가?", "현재 따르고 있지 않은 업무 방식 중 어떠한 업무 방식을 따라야 하는가?"

이전에 실시했던 CISO 평가인 *Finding a Strategic Voice*에서, IBM은 이러한 질문에 대한 답을 찾기 시작했습니다.[3] IBM의 분석가는 보안 책임자를 영향력이 있는 책임자(Influencer), 조직을 보호하는 책임자(Protector), 요구에 대응하는 책임자(Responder)라는 세 가지 유형으로 설명했으며, 각 유형의 책임자에 대한 전체적인 성숙도 및 특징을 분석했습니다. 이러한 분석을 통해, 더욱 성숙한 보안 책임자가 더욱 견고한 구조 및 관리 접근법을 이용할 때 조직의 접근 범위가 더 넓어지며 성과가 더욱 엄격하게 평가될 수 있다는 것을 밝혔습니다.

2013년도의 연구에서도 이와 유사한 패턴을 발견했으며, 더욱 심층적인 분석을 통해 핵심적인 결론, 우수 비즈니스 방식, 그리고 성숙한 보안 책임자조차 아직 해결하지 못한 부족한 점들을 밝혔습니다. 업무 방식, 기술 성숙도 및 평가 역량이라는 세 가지 영역을 심층적으로 살펴보면, 신임 보안 책임자 및 경험이 풍부한 보안 책임자 모두에게 지침이 될 수 있는 경로를 찾을 수 있을 것입니다.

비즈니스 방식:
의사소통을 통해 우려를 완화

초보 CISO에게 어떠한 조언을 해 줄 것인지, 향후에는 어떠한 기술이 중요할 것인지, 그리고 이해 당사자와의 신뢰를 구축하는 방법은 무엇인지에 대한 성숙한 보안 책임자들의 조언은 비슷했습니다. 성숙한 보안 책임자들은 강력한 비전, 전략 및 정책, 종합적인 리스크 관리, 그리고 효과적인 비즈니스 관계에 중점을 둘 것을 권고했습니다. 이들은 투명하고 신뢰할 수 있는 방법을 통해 활발한 의사소통을 함으로써 지속적으로 신뢰를 구축하고 있다고 답했습니다. 보안 책임자들은 기술 역량을 강화하고 비즈니스 감각을 확장하는 데 있어 이러한 활동이 매우 중요하다고 보고 있습니다.

"보안은 어려운 문제이며, 보안 담당자들은 각자만의 시각을 갖고 있습니다. 보안 담당자들은 '기술적인 혼동'을 피하기 위해 노력하지만, 이는 비즈니스 부서에서 중시하는 측면이 아닙니다. 비즈니스 부서는 명확한 사실을 요구하며, 이론적인 문제에는 관심이 없습니다."

— 보험 업계의 최고 기술 책임자

경험이 풍부한 보안 책임자가 말하는 '보안 책임자로서 성공하는 방법'

강력한 전략 및 정책	"보안 관련 의사결정을 할 때 중요한 것은 전략적 비전, 보안에 대한 위험 평가 및 우선순위 설정, 새로운 기술의 영향력에 대한 이해, 솔루션을 구별하고 가장 우수한 솔루션을 선택할 수 있는 역량의 확보입니다." (보험 업계의 IT 책임자)	"정책에 대하여 전반적인 일관성, 즉 하나의 프레임워크를 유지해야 합니다. 여기서 핵심은 프로세스입니다. 보안 프로세스의 일관성이 유지되지 않으면 사람들이 무엇을 해야 할지 혼란스러워하며 질문을 할 것입니다." (금융 서비스 업계의 IT 담당 부사장)
종합적인 위험 관리	"위험 평가 정보는 보안 정책을 결정할 때 이용됩니다. 위험 평가 정보는 언제, 어디서, 무엇을, 어떻게 보호하고 이러한 작업을 위한 비용, 즉 비즈니스 부서의 입장에서의 비용을 결정하는 데 도움이 됩니다." (제조 업계의 IT 그룹 책임자)	"전체적인 위험 관리를 위해서는 비즈니스를 이해해야 하며, 따라서 비즈니스 모델, 외부 관계자와의 접점, 규정 관련 프레임워크, 그리고 IT 위험만이 아닌 비즈니스 위험 등을 이해해야 합니다." (미디어 및 엔터테인먼트 업계의 최고 정보 책임자)
효과적인 비즈니스 관계	"판매를 위해서는 비즈니스 부서의 지원을 얻어야 합니다. 이 때는 비즈니스 전문 지식을 보유하고 있을 뿐만 아니라 기술에 대한 이해를 가지고 있는 사람이 필요하며, 이들은 비즈니스 가치에 대해 이야기하고 위험을 이해할 수 있습니다." (보험 업계의 최고 기술 책임자)	"비즈니스 부서와 함께 작업할 때 보안 책임자는 최대한의 투명성을 보이고, 비즈니스 사례 및 대안을 제시하고, 비즈니스 부서의 접근법과 일치하는 솔루션에 대해 이야기해야 합니다." (제약 업계의 IT 책임자)
의사소통을 위한 공동의 노력	"위험에 대한 완벽한 의사소통을 위해서는 다른 병원들이 현재 시행하고 있는 수많은 구체적인 사례를 제시해야 합니다. 비즈니스 부서에 뉴스 기사의 단편을 제공하고, 다른 병원에서의 보안 침해는 어떠한지 설명하고, 이와 관련된 벌금 및 과태료에 대해 설명해야 합니다." (헬스케어 업계의 최고 정보 책임자)	"효과적인 관계를 구축하기 위해서는 수많은 의사소통이 필요하며, 비즈니스 책임자에게 도움을 제공하고, 보안의 중요성을 전달하고, 보안 강화에 대한 장점을 설명하고, 위험을 설명하기 위해 회의 중에 자신의 시간을 요청해야 합니다. 이러한 배경 작업을 통해 사람들의 마음을 열 수 있게 됩니다." (공공 설비 업계의 인프라 책임자)

비즈니스 방식에 대한 과제: 다양한 비즈니스 관련 우려사항의 관리

많은 보안 책임자들은 CEO 등의 최고 경영진이 어떠한 관심사항을 가지고 있는지 이해하고 있으며, 이는 보안 책임자들이 조직 전체에 걸쳐 업무를 진행하고 의사소통하고 있다는 것을 나타내는 긍정적인 현상입니다. 성숙한 보안 책임자들은 이사진 및 최고 경영진들과 정기적으로 회의를 하는 경향이 높으며, 이를 통해 관계를 향상시킵니다. 그러나, 최고 경영진들은 보안과 관련된 가장 큰 우려사항에 대해 서로 다른 생각을 가지고 있습니다(그림 1). 인터뷰 대상자들의 답변에 따르면, CEO가 가장 민감하게 생각하는 문제는 브랜드 위상이나 고객의 신뢰에 악영향을 미치는 것이라고 말했습니다. CFO들은 보안 침해나 사고로 인한 재무적인 손실을 우려하고 있으며, COO들은 업무의 중단에 대해 걱정하고 있습니다. 마지막으로, CIO들은 광범위한 관심사항을 가지고 있으며, 여기에는 보안 침해, 데이터의 손실 및 기술 투자의 실행 등이 포함됩니다.

	브랜드 위상/신뢰의 손실	재무적 손실	업무의 중단	규정 준수 위반	기타
CEO	49%	6%	15%	9%	21%
CIO	26%	0%	24%	18%	32%
CFO	14%	47%	6%	21%	12%
COO	38%	4%	42%	8%	8%
평균	32%	14%	22%	14%	18%

그림 1 – 보안 책임자들에 따르면, 최고 경영진들은 보안과 관련된 가장 큰 문제에 대해 서로 다른 생각을 가지고 있는 것으로 나타났습니다.

경영진들의 우려사항이 이렇게 다양하기 때문에 까다로운 과제가 발생합니다. 인터뷰에 응한 보안 책임자들은 이러한 다양한 우려사항을 완화시키기 위해 이사진 및 최고 경영진들과 정기적으로 회의를 하며, 분기당 한 번씩 회의를 하는 경우가 가장 많았습니다. 회의 시에 논의하는 가장 중요한 주제에는 리스크의 식별 및 평가(59%), 예산 관련 문제 및 요청의 해결(49%) 및 새로운 기술의 배치(44%)가 포함되었습니다. 리스크에 초점을 두는 것은 좋은 현상이며, 이러한 회의를 통해 보안 책임자들은 최고 경영진들이 가지고 있는 다양한 우려사항을 모두 처리할 수 있는 기회를 얻습니다.

보안 책임자들이 브랜드 위상이나 고객의 신뢰에 대한 손실이 조직 전체에 걸쳐 가장 중요한 비즈니스 우려사항이라고 생각하고 있다는 사실은 흥미로운 문제를 제시합니다. 보안 침해 및 기타 사고가 주식 가격이나 대중의 인식에 영향을 미칠 수는 있지만, 보안 침해나 사고가 브랜드의 위상에 미치는 영향을 추적하는 것은 현재로서는 거의 불가능합니다. 인터뷰에 응한 보안 책임자 중 이러한 영역의 역량을 갖춘 보안 책임자는 거의 없었습니다. CEO의 우려사항은 궁극적으로 브랜드 위상 및 고객의 신뢰에 중점을 둘 수도 있지만, 실질적으로 가능한 것이 무엇인지 최고 경영진들에게 현실적으로 설명하기 위한 비즈니스 및 의사소통 역량을 보유하는 것은 보안 책임자의 몫입니다. 이는 확실히 업계 전체가 발전시켜야 할 영역입니다.

CISO의 관점:
비즈니스 책임자들에 대한 균형 조정

의견 제공: Shamla Naidoo
정보 리스크 및 보안 담당 부사장
Starwood Hotels & Resorts Worldwide, Inc.

Starwood는 자산과 직원 및 고객의 데이터를 적극적으로 보호할 수 있도록 보장하기 위해 최고 경영진들과 이사진의 검토 및 승인 하에 종합적인 보안 전략을 개발해 왔습니다. Starwood의 책임자들에게 업계의 변화 및 증가하는 위협에 대한 정보를 지속적으로 제공하기 위해 IT 보안 팀은 전략 및 잠재적인 보안 리스크에 대한 경과 보고서를 정기적으로 제공합니다. 급속하게 변화하는 비즈니스 환경에서, 서비스 업계는 서비스 지향적인 특성으로 인해 보안에 대한 인식이 크게 높아지고 있습니다. 이에 대한 건전한 논의와 솔직한 대화가 이루어지고 있으며, 이는 신중하면서도 신속한 의사결정으로 연결되어 업계의 발전과 보안 리스크의 적절한 관리를 보장하도록 돕고 있습니다.

제가 신임 보안 책임자에게 할 수 있는 가장 좋은 조언은 다음과 같습니다.

1. 보안 전략을 수립하고 목표와 계획에 대해 이사진의 동의를 얻으십시오.
2. 실제적인 경험에 대한 교육을 제공하거나, 이를 위해 외부 인력을 고용하십시오. 보안을 유지하는 방법을 모른다면 보안을 지킬 수 없습니다.
3. 끊임 없이 변화하는 보안 리스크를 지속적으로 확인하고, 보안 관련 의사결정을 할 때는 법적인 문제를 고려하십시오.
4. 해당 기업이 어떻게 수입을 창출하고 있는지 이해한 후, 기업의 성장 및 혁신에 영향을 미칠 수 있는 리스크를 관리하고 기업의 수입 창출을 적극적으로 지원하기 위한 생산적인 방법을 모색하십시오.
5. 비즈니스 이해 당사자와의 의사소통을 통해 잠재적인 리스크와 솔루션에 대한 정보를 제공하여 이들이 보안 업무를 도울 수 있도록 하십시오.

"보안 책임자는 비즈니스 기술과 소비자 기술의 최첨단에 서 있어야 합니다. BYOD에 거의 모든 것이 포함되기 시작했으며, BYOD 장치는 점차 확산되고 있습니다. 보안 책임자들은 스마트해야 하며, 지식을 갖추어야 합니다.
사용자와 동일하게 생각하고, 사용자가 무엇을 하는지에 대해 생각해야 합니다."

— 금융 서비스 업계의 최고 정보 책임자

기술:
기본적인 기술을 넘어서

보안 책임자들의 초점은 리스크 관리, 더욱 강력한 비즈니스 관계 및 더 나은 의사소통으로 이동하고 있지만, 보안 기술은 보안 책임자 전체에게 여전히 매우 중요한 도구입니다. 실제로, 인터뷰 대상자들은 기술을 평가하는 데 상당한 시간을 보내고 있습니다(24%, 전체 영역 중 1위).

많은 보안 책임자들은 기본적이고 기능적인 보안 기술이 조직의 가장 핵심적인 구성요소인 것으로 생각하고 있습니다. 이러한 기술에는 기업의 신원 및 액세스 관리(51%), 네트워크 침입 방지 및 취약성 스캐닝(39%), 그리고 데이터베이스 보안(32%)이 포함됩니다. 중요성의 측면에서, 가장 발전된 또는 가장 전략적인 기술은 기본적인 기술을 추월하지 못했으며, 이러한 기술에는 고급 악성코드 발견(20%), 보안 인텔리전스 분석(15%) 및 대안적인 인증 메커니즘(12%)이 포함됩니다. 향후에 이러한 상황이 어떻게 바뀔지 확인하는 것은 흥미로운 일이 될 것입니다.

잘 알려진 우려사항에도 불구하고, 보안 책임자들은 모바일 보안의 구현 및 클라우드 기반 보안 서비스 도입을 빠르게 진행하고 있습니다. 모바일 보안은 "가장 최근에 배치된" 보안 기술 중 1위를 기록하고 있으며, 지난 12개월 동안 25%의 보안 책임자가 모바일 보안 기술을 배치했습니다. 그리고 클라우드 환경에서의 개인 정보 및 보안에 대한 우려는 여전히 남아 있지만, 보안 책임자 중 약 4분의 3(76%)은 어떠한 형태로든 클라우드 보안 서비스를 배치했으며, 가장 많이 배치된 기능은 데이터 모니터링 및 감사 기능, 그리고 페더레이티드(federated) 신원 및 액세스 관리(두 항목 모두 39%)였습니다.

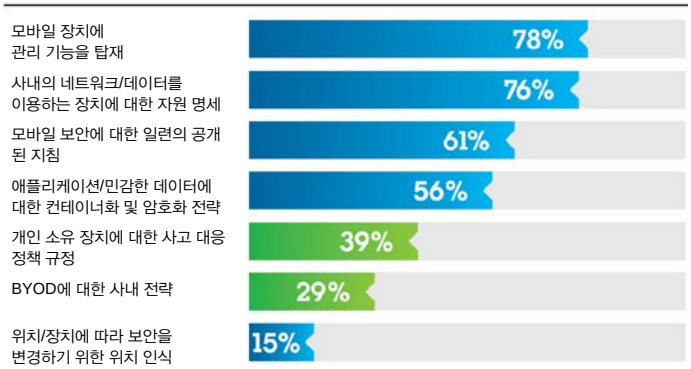
많은 수의 인터뷰 대상자는 보안에 대한 기초를 강화하면서도 더욱 고급화된 기술을 천천히 테스트하여 클라우드 및 모바일 기술을 구축하고 있었습니다. 보안 책임자는 모든 새로운 기술을 뒤쫓아서는 안 되며, 현재 이용 중인 접근법을 혁신하고 비즈니스 목표를 발전시킬 수 있는 기술에 집중해야 합니다.

기술에 대한 과제: 모바일 보안의 모든 측면에 대한 강화

2012년도 CISO 평가에서는 모바일 보안이 가장 큰 기술적 관심사항이었으며, 지난 2년 동안 50% 이상의 보안 책임자는 모바일 보안이 주요 기술 과제라고 응답했습니다. 모바일 보안은 지속적으로 큰 관심을 받고 있으며, 14개의 서로 다른 기술 분야 중에서 모바일 보안은 지난 12개월 동안 "가장 중요한 기술"이자 "가장 많이 배치된 기술"인 것으로 나타났습니다. 모바일은 가장 중요한 관심사항이며 투자 지원을 받고 있지만, 모바일 기능은 아직 성숙한 기술이 아닙니다.

현재, 모바일 보안은 개발의 기초 단계에 있습니다. 가장 높은 빈도로 배치되는 사례는 장치에 모바일 장치 관리 기능을 탑재하는 것(78%)과 사내의 네트워크 또는 데이터를 이용하는 장치에 대한 자원 명세를 관리하는 것(76%)이었으며, 이는 사내에 모바일 기술을 안전하게 구축할 때의 첫 번째 단계에 해당합니다(그림 2).

배치된 기능



가장 중요한 기능

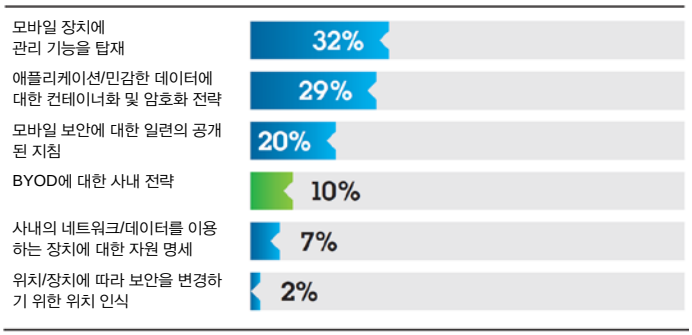


그림 2 – 모바일 보안 정책 및 전략에 대한 우선순위는 아직 낮습니다.

보안 책임자가 직면하고 있는 모바일 관련 주요 과제는 초기 단계 이상으로 진행하는 것과 기술보다는 정책 및 전략에 더 많은 초점을 두는 것입니다. 인터뷰 대상자의 대부분은 개인 소유 장치에 대한 종합적인 모바일 정책 및 전략을 아직 널리 이용하고 있지 않았거나 이를 중요하지 않은 것으로 생각하고 있었습니다. 40% 미만의 조직이 개인 소유 장치에 대한 구체적인 대응 정책, 즉 BYOD에 대한 사내 전략을 실행하고 있었으며, 매우 소수의 조직만이 이러한 행동을 "가장 중요"한 것으로 생각하고 있었습니다.

그러나 보안 책임자들은 이러한 격차를 인지하고 있으며, 이 문제를 해결하는 중입니다. BYOD에 대한 사내 전략(39%) 및 개인 소유 장치에 대한 사고 대응 정책(27%)은 향후 12개월 동안 개발할 예정인 영역 중 가장 높은 순위의 영역이었습니다.

CISO의 관점:
신뢰의 구축을 통한 우려사항의 완화

의견 제공: Ken Kilby, 최고 정보 보안 책임자
BB&T

BB&T는 설립된 지 141년 된 은행으로, 앞으로도 그 역사만큼 지속적으로 운영될 것입니다. 이를 위해 저희는 보안 및 리스크에 대해 하나의 팀으로 접근하고 있으며, 보안과 리스크는 모두의 책임입니다. 가장 중요한 점은, BB&T의 구성원 모두가 BB&T라는 이름을 갖는다는 것입니다. 고객사와 고객에 대해 안전한 액세스를 유지하지 못한다면 직무를 다하지 못한 것입니다. BB&T의 통제 및 정책은 궁극적으로 위상에 초점을 두어야 합니다.

이러한 목표를 달성하기 위해, 저는 최고 경영진들 및 이사진과의 신뢰를 구축하는 데 많은 시간을 보냅니다. 지속적으로 이사진과 경영 팀의 각 구성원과 연락하여 인간 관계를 발전시키고 있습니다. 최고 경영진들은 서로 다른 우려사항을 가지고 있으며, 저는 이러한 우려사항을 해결해야 합니다.

BYOD는 저희에게도 큰 관심사항입니다. 저희는 최신 기술을 따르기 위해 노력하고 있지만, 항상 가장 중요한 최신 기술에 대한 격차를 좁히고 있을 뿐인 것처럼 느껴집니다. 저희는 많은 수의 다양한 모바일 플랫폼을 관리 및 보호해야 하며, 과다한 악성코드가 발생한 경우에는 처리하기가 매우 어렵습니다.

동료 보안 책임자 여러분께 권장하고 싶은 지침은 두 가지입니다. 첫 번째는, 보안 책임자는 자신의 역량을 발전시켜야 한다는 것입니다. 보안 책임자는 이사진이 이해할 수 있는 언어로 의사소통할 수 있어야 합니다. 항상 활발한 의사소통을 하고, 일상적인 업무에 지나치게 파묻히지 마십시오. 두 번째는 제 업무에 필수적인 것으로, 사법 기관, 업계의 파트너 및 입법자와의 관계를 발전시켜야 한다는 것입니다. 공적인 의사소통과 사적인 의사소통을 더욱 많이 하게 되면 궁극적으로 전체적인 공격 취약점이 감소할 것입니다. 여러 명이 협력하면 더 많은 일을 할 수 있습니다.

평가:
적절한 피드백 루프의 형성

현재, 보안 책임자들은 주로 예산 설정에 대한 지침 및 새로운 기술에 대한 투자 사례를 위해 지표를 이용하고 있습니다. 일부 경우에는 평가를 통해 보안 조직에 대한 전략적 우선순위를 설정하고 있습니다. 그러나 일반적으로 기술적 지표 및 비즈니스 지표는 여전히 운영 관련 문제에 초점을 두고 있습니다. 예를 들어, 인터뷰 대상 중 90% 이상은 보안 사고, 기록, 데이터 또는 장치의 분실이나 도난, 그리고 감사 및 규정 준수 현황을 추적하고 있으며, 이는 모든 보안 책임자가 추적할 만한 기본적인 수준의 업무입니다. 소수의 응답자(12%)들이 비즈니스 지표 및 보안 지표를 사내의 리스크 프로세스에 피드로 제공하고 있었으며, 이는 보안 책임자들이 보안이 전체적인 사내 리스크에 미치는 영향이 성공을 위해 가장 중요한 요인이라고 말한 것과는 대조되는 것입니다.

"저희는 지표를 이용해 지속적으로 프로세스를 개선하고 인식을 향상시키고 있습니다. 지표는 경쟁에서 앞서기 위해 앞으로 무엇을 해야 할지 결정하는 데 도움이 됩니다."

— 금융 서비스 업계의 IT 담당 부사장

평가에 대한 과제:
보안 지표를 비즈니스 언어로 변환하기

지표를 사내 리스크 프로세스에 피드로 제공하는 것의 중요성에 대한 인식과 이에 대한 실제 행동 사이의 차이는 CISO 및 보안 책임자가 직면한 과제를 반영합니다. 2012년도 CISO 평가에서는 더욱 성숙한 보안 책임자들이 더 많은 항목을 더 높은 빈도로 평가한다는 것을 확인했습니다(예: 교육 및 훈련, 리스크 등). 하지만 이러한 정보를 이용해 무엇을 해야 할까요? 그리고 이러한 정보를 비즈니스 부서에 어떻게 전달하여 조치를 취하도록 할 수 있을까요?

보안 책임자 중 약 3분의 2는 지표를 재무적 성과로 변환하고 있지 않습니다. 이들에게는 지표의 변환을 위한 자원이 부족하거나, 지표를 변환하도록 하는 비즈니스 요구사항이 존재하지 않거나, 또는 이러한 지표가 너무 복잡하여 계산하지 못하고 있습니다. 또한, 50% 이상의 보안 책임자는 보안 지표를 비즈니스 리스크에 대한 측정치와 완전히 통합하지 않고 있습니다(그림 3). 성과와 관련된 지표들을 통합하지 않는 경우에는 이로 인해 보안 책임자가 다른 비즈니스 책임자와 의사소통할 수 있는 역량에 제약이 가해질 수 있으며, 따라서 내부적으로 조직의 상태를 효과적이고 정확하게 설명하기 어려워집니다.

CISO의 관점:
비즈니스 이점의 평가

의견 제공: Felix Mohan, 부사장 겸
글로벌 최고 정보 보안 책임자
Bharti Airtel Limited

최초에 저희는 지표 평가 프로그램을 훨씬 더 운영적이고 전략적인 관리 수준에서 시작했습니다. 이는 원가 중심점으로써의 필요 자원에 대한 정당성을 증명하기 위한 것이었습니다. 점점 더 많은 것을 학습하고 점점 더 성숙해짐에 따라서, 더욱 전략적으로 변모하기 위해 평가 방법을 변경했으며, 리스크, 규정 준수, 비즈니스 연속성, 인식 및 교육, 그리고 중요 애플리케이션의 가동 시간 등의 항목을 추가했습니다.

현재, 저희는 여전히 지표 프로세스를 향상시키고, 자동화를 시도하고, 전사적인 리스크 수준을 확인하고, 보안 지표를 비즈니스에 대한 영향으로 변환하는 작업을 진행하고 있습니다. 저희는 비즈니스 리스크 허용치를 더욱 잘 이해하고, 이러한 값을 평가하는 방법을 이해하기 위해 지속적으로 노력하고 있습니다.

최근의 평가 작업의 일환으로, 저희는 제품 및 서비스의 기반이 되는 모든 중요 프로세스, 즉 회사에 대한 수입을 창출하는 모든 것을 식별했습니다. 저희는 이러한 프로세스가 의존하고 있는 모든 IT 및 기술 인프라를 식별했습니다(예: 시스템 및 애플리케이션, 중요 자산). 또한, "이러한 프로세스 및 자산을 이용할 수 없는 경우에는 복구 시간이 얼마나 걸릴 것인가?"라는 질문에 대한 답을 찾았습니다. 그 후에는 이러한 프로세스를 매우 민감, 중요도 높음, 중요도 중간 및 중요도 낮음으로 분류했습니다. 이러한 분류에 따라 해당 인프라를 얼마나 빨리 복구해야 할지 결정하며, 복구 기간은 몇 시간에서 며칠 사이입니다.

재무적 영향의 평가

"재무적 영향의 평가는 기술을 구현할 때 중요한 역할을 합니다. 이는 ROI는 얼마이며, 사고에 대한 비용 회피는 얼마인가에 대한 답을 제공합니다. 저희는 이러한 측정치를 이용해 가치가 존재하는지의 여부를 증명합니다."(보험 업계의 최고 기술 책임자)

IT 지표와 비즈니스 리스크 지표의 통합

"보안 지표는 고객 만족도와 결합되며, 이는 더 넓은 범위의 연속성 및 비즈니스 영향 분석에 포함됩니다. 사이버 보안은 위험 분석 및 다른 문제에 통합됩니다." (공공 설비 업계의 IT 책임자)

그림 3 – 재무적 영향의 평가, 그리고 보안과 리스크의 통합이 부족하다는 것이 명확히 드러났습니다.

더욱 다양한 성과를 올리는 보안 책임자가 되는 방법

이러한 통찰력과 과제는 우리에게 정보 보안 책임자의 초점과 접근법에 대해 무엇을 알려 주고 있을까요? 이러한 통찰력과 과제를 통해 진행 상황의 평가를 위한 모델을 구성하거나, 따라야 할 경로를 찾을 수 있을까요?

시작 단계에 있는 보안 책임자의 경우, 이러한 통찰력과 과제는 IT 보안이 미치는 경제적인 영향을 고려한 전체적인 리스크 관리에 강력한 보안 전략을 결합하고, 효과적인 비즈니스 관계를 발전시키고, 고위급 책임자에 대한 신뢰를 형성하도록 제안합니다. 보안 책임자는 기본적인 보안 기술을 유지해야 하지만, 더욱 고급화되고 전략적인 기능도 소홀히 해서는 안 됩니다. 또한, 정책을 중시하고 개인 소유 장비의 이용이 가능하도록 하는 종합적인 모바일 보안 접근법을 이용해야 합니다.

또한, 보안 책임자는 적절한 피드백 루프를 생성해야 합니다. 보안 기술 및 비즈니스 지표는 모두 리스크 관리 프로세스에 피드로 입력되어야 하며, 이는 단순히 항목으로서 입력되는 것이 아니라 심층적인 통합을 통해 입력되어야 합니다. 이러한 지표는 해당 조직에서 이용하는 언어로 변환되어야 합니다. 그렇지 않으면 보안을 통해 비즈니스 계획을 실행할 수 없으며, 조직 전체에 걸쳐 보안 프로젝트에 대한 지출의 필요성을 합리화하기 어려워집니다.

CISO가 더 높은 성과를 올릴 수 있는 계획의 수립

인터뷰에 응한 일부 보안 책임자는 다른 보안 책임자보다 이러한 융통성 모델에 더욱 가까웠으나, 이러한 모델에 포함된 모든 사항을 실천하고 있는 보안 책임자는 거의 없었습니다. 비즈니스 방식, 기술 및 평가 역량의 적절한 조합을 이용하여 핵심 과제를 처리하고 있는 보안 책임자는 보안 책임자의 성숙도에 대한 새로운 기준을 세웠습니다. 이들은 조직 내에서의 정보 보안의 역할을 혁신하고 있습니다. 이들은 기술 및 비즈니스 모두와 관련된 여러 규정에 대한 숙련도를 보이고 있으며, 보안 책임자들 사이에서 빠른 속도로 널리 이용되고 있는 기술을 발전시키고 있습니다.

추가 정보

ibm.com/ibmcai/ciso를 방문하면 보안 책임자의 역할 변화에 대한 추가 정보를 확인할 수 있습니다.

비즈니스 방식

필수 단계

CISO로서의 역할을 공식화하여 조직에서의 권위와 예산에 대한 권한을 갖춘 한 명의 고위급 보안 책임자로서 인정받도록 하십시오.

조직 내의 다른 전략(예: 제품 개발, 리스크 및 성장)을 함께 고려하여 **보안 전략을 수립**한 후 정기적으로 업데이트하고 널리 전달하십시오.

최고 경영진들 및 이사진과의 **효과적인 비즈니스 관계를 발전**시키고, 이들과 높은 빈도로 회의하고, 이들의 여러 가지 우려사항을 관리하기 위한 접근법을 개발하십시오. 평가 대상을 결정할 때는 이러한 우려사항을 고려하십시오.

투명하고 신뢰할 수 있는 방법을 통해 높은 빈도로 비즈니스 이해 당사자와 의사소통하여 **신뢰를 구축**하십시오.

기술

필수 단계

고급 기술을 통해 비즈니스 목표를 달성할 수 있는 경우에는 **고급 기술에 투자**하십시오. 기본적인 보안 기술에 모든 자원을 소비하지 말아야 하며, 기존의 접근법을 혁신할 수 있는 고급 기술 및 방법을 모색해야 합니다.

기술만을 이용하는 것이 아니라 일련의 비즈니스 방식 및 정책 또한 이용하여 개인 소유 장비 및 기업 소유 장비 모두에 대한 **모바일 보안을 강화**하십시오.

업계의 동료를 포함한 다른 그룹과 **정보를 공유**하십시오. 이를 통해 기술 투자 시에 확실성을 높이고 보안 우선순위 및 우수 사례에 대한 질문에 답할 수 있습니다.

평가

필수 단계

단순한 감사 및 규정 준수에 초점을 두는 것이 아니라, **리스크가 미치는 전체적인 경제적 영향에 초점**을 두십시오. 기업을 보호하기 위한 방법을 결정하고 보안이 브랜드 가치 및 위상에 미치는 영향을 이해하십시오.

이사진 및 최고 경영진들에게 무엇을 실행 가능한지 현실적으로 설명하여, 이들이 가지고 있는 **위상에 대한 리스크 및 고객 만족도와 관련된 우려사항을 처리**하십시오

지표를 재무적 영향으로 **변환**하고 IT 및 비즈니스 리스크 지표를 완전히 통합하십시오.

그림 4 – 더욱 강력한 보안 책임자가 되기 위한 필수 단계.

저자 소개

Marc van Zadelhoff, 전략 및 제품 관리 담당 부사장, IBM Security Systems

전략 및 제품 관리 담당 부사장인 Marc van Zadelhoff는 IBM의 글로벌 보안 소프트웨어 및 서비스 포트폴리오에 대한 전체적인 오퍼링 관리, 예산 설정 및 포지셔닝을 담당하고 있습니다.

이메일 주소: marc.vanzadelhoff@us.ibm.com.

Kris Lovejoy, 총괄 매니저, IBM Security Services

총괄 매니저 Kris Lovejoy는 보안에 대한 매니지드 서비스 및 전문 서비스의 개발과 이러한 서비스를 전 세계의 IBM 고객에게 제공하는 업무를 담당하고 있습니다. 이전에는 IBM의 정보 기술 리스크 및 글로벌 CISO 담당 부사장으로 글로벌 기업 보안 및 복원 기능 관리, 모니터링 및 테스트를 담당하였습니다.

이메일 주소: klovejoy@us.ibm.com.

David Jarvis, 매니저, IBM Center for Applied Insights

David Jarvis의 전문 분야는 새로운 비즈니스 및 전략적 기술 주제에 대한 사실 기반의 연구입니다. David Jarvis는 *다음 세대를 위한 사이버 보안 교육*(*Cybersecurity Education for the Next Generation*)을 포함한 IBM의 여러 보안 연구와 2012년도 IBM CISO 평가에서 공동 저자로 활약하였습니다.

이메일 주소: djarvis@us.ibm.com.

도움 주신 분들

Caleb Barlow, *모바일 보안, 애플리케이션 보안, 데이터 보안 및 중요 인프라 보안 책임자*

David Puzas, *글로벌 마케팅 이사, IBM Security Services*

Adam Trunkey, *글로벌 마케팅 매니저, IBM Security Services*

IBM Center for Applied Insights 소개

ibm.com/ibmcai

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

참조 정보

[1] Gottlieb, Joe. “Being great: Five critical CISO traits.” *SC Magazine*. June 13, 2013. http://www.scmagazine.com/being-great-five-critical-ciso-traits/article/298686/

[2] Ashford, Warwick. “CISOs must shape up or ship out, says Forrester.” *ComputerWeekly.com*. June 11, 2013. http://www.computerweekly.com/blogs/david_lacey/2013/07/where_next_for_the_enterprisin.html

[3] *Finding a strategic voice: Insights from the 2012 IBM Chief Information Security Officer Assessment*. IBM. May 2012. http://www-01.ibm.com/ common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=CIE03117USEN

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2013

CIW03087-USEN-00