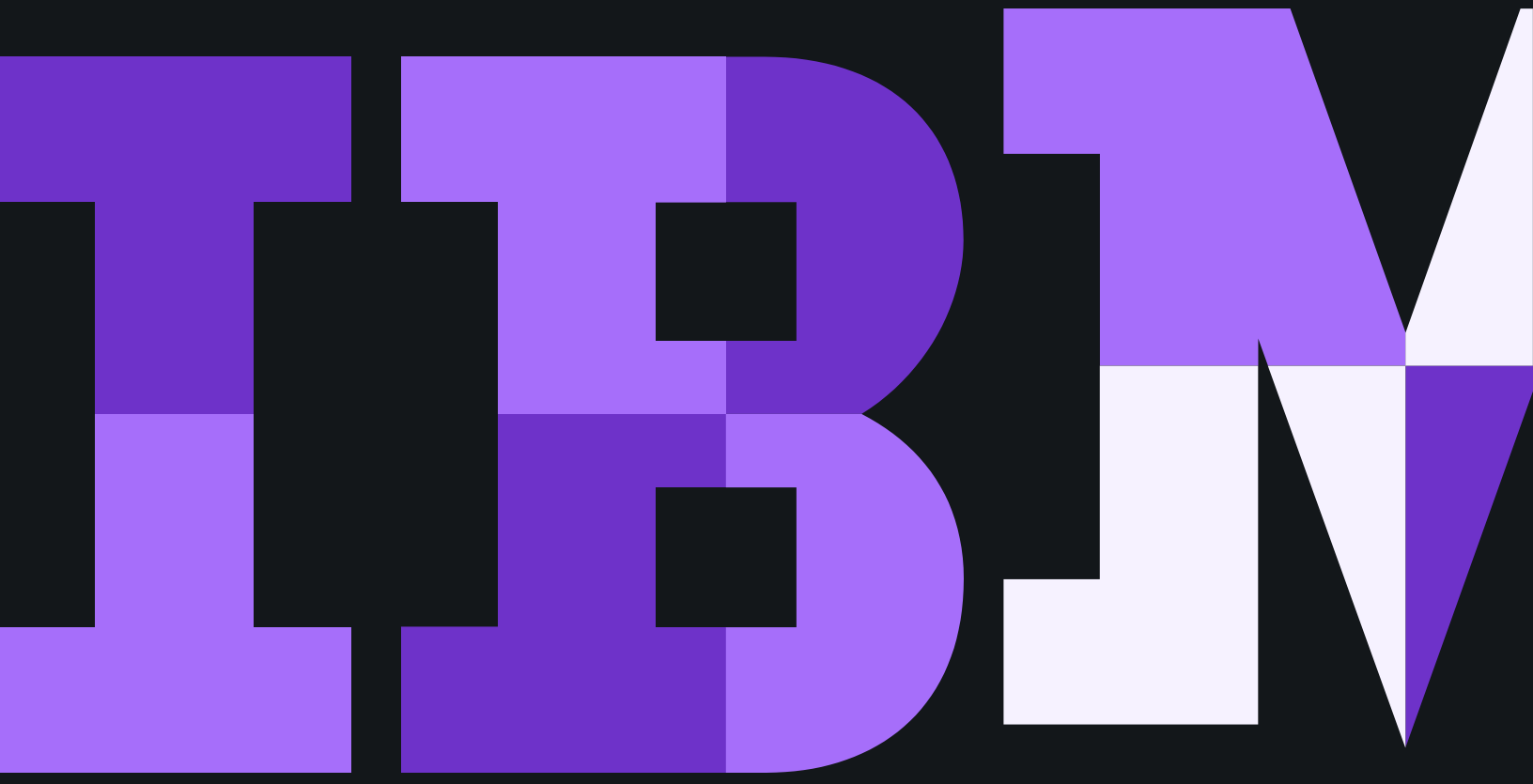
IBM Security

2020년 1월

# 사이버 보안 위험 관리를 위한 전략

## 보안 및 규제 준수 상태 평가와 개선



IBM

## 목차

## 현재의 사이버 보안 환경

데이터 침해, 랜섬웨어 공격, 개인정보 유출, 기타 사이버 보안 관련 문제에 모두가 관심을 갖고 있지만 대부분의 기업은 여전히 이러한 문제에 효과적으로 대비하지 못하고 있습니다. 많은 조직이 분명하고 적절한 보안 전략을 가지고 있지 않고 사이버 보안 성숙도에 대한 인사이트가 부족하며 사이버 보안 인시던트에 대응하기 위한 계획이 있다하더라도 충분히 활용하지 못합니다. 사실상 대다수 조직의 위험 관리 방식이 상당히 위험한 수준이라고 할 수 있습니다.

조직은 IT 위험을 높이는 부정적 요인에 직면하는 경우가 많습니다. 그 예로는 인수, 합병, 매각, 클라우드, IoT, 퀀텀과 같은 새로운 기술과 규제 변화 등이 있습니다. 이와 동시에 조직은 보안 및 규제 준수 문제를 해결하면서 혁신을 통해 앞으로 나아가야 합니다. 기업의 발전을 저해하는 문제의 예는 다음과 같습니다.

- 복잡한 규제 요구사항
- 적절하게 조율된 보안 전략, 사이버 보안 및 규제 준수 성숙도 결여
- 잦은 조직적 변화
- 보안 스킬 부족
- 보안 “베스트 프랙티스”를 둘러싼 불확실성

**279일**

보안 침해 행위를 발견하고 억제하는 데 걸리는 시간(전 세계 평균)

**25,575개의 레코드**

데이터 침해 규모(전 세계 평균)

**비즈니스 손실**

데이터 침해로 인한 비용을 유발하는 가장 큰 요인[1]

## 위험에 대한 조치 실행

변화하는 사이버 보안 위협과 규제에 보조를 맞추어 대응하는 일은 어렵습니다. 많은 기업이 사이버 불확실성에 직면하여 사이버 보안 및 규제 준수 상태에 대한 이해를 높이고 베스트 프랙티스를 배우며 비즈니스 목표를 추구하기 위해 신뢰할 수 있는 어드바이저의 지원을 활용합니다. 신뢰할 수 있는 어드바이저가 있으면 운영 중단을 더욱 효과적으로 예측하여 변화하는 보안 환경에 적응하고 새로운 혁신을 추구하며 보안의 중요성을 간과하지 않고 경쟁 우위를 차지할 수 있습니다.

앞서가는 조직은 조직의 현 상황에 대한 정확한 벤치마크를 얻고 위험, 규제 준수, 거버넌스를 더 효과적으로 관리하기 위한 계획을 개발합니다. 이러한 평가 활동에는 위험 정량화, 타사 보안 위험 식별, 자사 시스템의 약점을 찾아내는 침투 테스트, 그리고 직원과 기술을 테스트하고 요구사항을 파악하고 사이버 공격에 대한 자동적 대응을 구축하기 위한 사이버 침해 시뮬레이션 등이 있습니다.

사이버 레인지(cyber range, 가상 훈련장)는 앞서가는 조직의 위험 관리 전략의 일부로 부상하고 있습니다. 사이버 레인지를 통해 조직은 보안 팀과 주요 임원이 통제된 환경에서 시뮬레이션된 보안 침해를 경험하도록 지원할 수 있습니다. 사이버 레인지에서의 훈련을 통해 조직은 인시던트 대응 계획에서 부족한 부분을 평가하고 보안 팀과 규제 준수 팀이 조직 전반에서 인시던트 대응을 어떻게 통합해야 하는지를 비판적으로 평가할 수 있습니다.

IBM과 함께 사이버 공격 대비 수준을 테스트한 Finastra

런던에 소재한 세계 최대의 금융 기술 기업 중 하나인 Finastra는 대륙 간 데이터 침해 행위에 대처하는 능력을 테스트하기 위해 IBM Security과 함께 사이버 레인지 이벤트에 참여했습니다.

비디오 보기

## 보안 위험 관리의 구성 요소: 평가, 감소, 관리

보안 위험을 최소화하려면 약점을 알고 이를 해결하는 방법을 찾아야 합니다.

현재의 사이버 보안 및 규제 준수 상태 평가

위험을 가장 잘 줄이는 방법 결정

향후 위험 노출 관리

이러한 종류의 보안에 대한 성찰에는 경험이 풍부한 외부적 관점을 활용하면 큰 도움이 됩니다. 즉, 적절한 문제 제기를 하고 성공을 위한 검증된 접근법을 통해 성과를 낼 수 있도록 도움을 주는 신뢰할 수 있는 어드바이저를 활용하는 것이 좋습니다. 숨어 있는 보안 취약점은 반드시 찾아내야 합니다. 이러한 취약점은 데이터 침해, 규제 준수 실패 혹은 회사의 평판과 수익에 악영향을 끼칠 수 있는 기타 위험에 비즈니스를 노출시킬 수 있기 때문입니다.

보안 어드바이저는 수많은 경험과 업계 베스트 프랙티스를 바탕으로 입증된 방법을 사용하여 위험을 파악하고 이러한 위험을 줄일 수 있는 해결책을 찾아내도록 도움을 줄 수 있습니다.

보안은 계속되는 도전과 같습니다. 어드바이저는 뛰어난 보안 및 규제 준수 태세를 유지하고 보안 문화를 장려하며 새로운 위협을 해결하고 시간이 흐름에 따라 보안 및 규제 준수 프로그램을 조정할 수 있도록 지속적인 보안 모니터링, 관리, 교육을 제공할 수 있습니다.

성공적인 보안 전략은 위에서 시작되어야 합니다. 신뢰할 수 있는 어드바이저는 리소스의 우선순위를 정하고 의사결정을 비즈니스 목표에 맞게 조정하며 가장 중요한 보안 및 규제 준수 이니셔티브에 대한 경영진의 지지를 공고히 하도록 조언을 제공할 수 있습니다. 여기에는 보안이 디지털 전략과 혁신 이니셔티브를 구성하는 필수 요소인 클라우드, IoT, 모바일 및 기타 이니셔티브가 포함됩니다.

신뢰할 수 있는 어드바이저는 리소스의 우선순위를 정하고 의사결정을 비즈니스 목표에 맞게 조정하며 경영진의 지지를 공고히 하도록 조언을 제공할 수 있습니다.

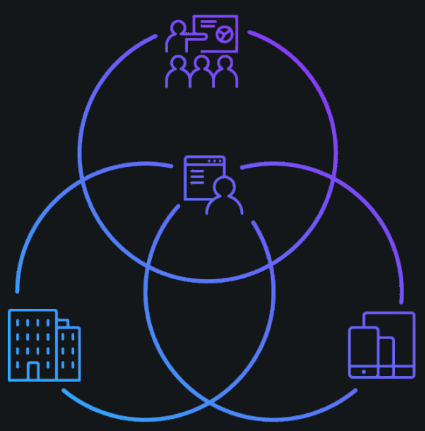
## 예기치 못한 상황에 대처

위험은 어디에나 존재합니다. 회사 밖에는 데이터를 훔치는 동안 사용자의 주의를 딴 데로 돌리도록 설계된 숨겨진 랜섬웨어와 무차별 대입 공격의 형태로 위험이 도사리고 있습니다. 회사 안에서는 신뢰할 수 있는 ID 뒤에 숨어 있거나 사람의 단순한 실수로 초래될 수 있습니다. 그리고, 자동화된 공장부터 AI 기반 고객 지원 센터까지 여러 가지 기회가 드리우는 그림자에 가려져 있을 수도 있습니다.

위험을 밝혀내고 이를 공개적으로 알리려면 신뢰할 수 있는 어드바이저가 필요합니다. 거버넌스, 위험 및 규제 준수 관리를 개선하려면 조직 내 위험에 대해 신뢰할 수 있는 견해가 필요합니다. 사이버 공격의 희생자가 될 때까지 사이버 공격의 희생자가 될 것이라고 예측할 수 있는 사람은 없습니다. 보안 어드바이저는 위험을 찾아내고 정량화하고 우선순위를 지정한 다음 관리하도록 도움을 줄 수 있습니다.

안정적인 위험 관리는 한 사람 또는 한 팀만의 책임이 아닙니다. 이를 위해서는 사업부, 리더, 프로세스를 포괄하여 모든 개인, 기계, 조직의 구성 요소를 고려하는 체계적이고 잘 조율된 접근법이 필요합니다.

안정적인 위험 관리를 위해서는 사업부, 리더, 프로세스를 포괄하여 모든 개인, 기계, 조직의 구성 요소를 고려하는 체계적이고 잘 조율된 접근법이 필요합니다.



## 신뢰할 수 있는 IBM Security

IBM Secruity와 함께라면 혼자서 위험과 싸우지 않아도 됩니다. IBM의 서비스는 적합한 보안 및 규제 준수 기능을 제공하여 프로세스, 사람, 기술 전반에 걸쳐 위험을 효과적으로 관리하도록 지원합니다. 새로운 위협 벡터, 새로운 규제 요건 또는 예기치 못한 상황 때문에 보안 환경이 바뀌는 경우에도 IBM의 보안 전문가 팀이 위험을 통제할 수 있도록 지원합니다.

IBM Security의 보안 전문성을 활용하면 효과적인 보안 전략을 세우는 동시에 조직 전체에서 보안 및 규제 준수 상태를 비판적으로 평가하고 역량(예: 데이터 침해에 얼마나 신속하게 대응할 수 있는지)을 정확히 측정하여 통제 체계(chain of control)에서 약한 연결 고리를 찾아낼 수 있습니다. IBM Security는 고객이 위험을 평가하고 감소시키고 관리할 수 있도록 지원하는 데 적합한 인력, 방법, 경험을 보유하고 있습니다. 그 예는 다음과 같습니다.

IBM Security Strategy Risk and Compliance 서비스(SSRC): IBM은 고객사의 목표를 기준으로 현재의 보안 거버넌스를 평가하도록 지원하고 고객이 위험 관리 전략과 프로그램을 개발할 수 있도록 안내를 제공하며 보안 성숙도 향상을 위한 고객의 노력을 지원합니다. IBM과 협력하면 다음과 같은 방법을 통해 위험, 규제 준수 및 거버넌스를 더 효과적으로 관리할 수 있습니다.

- C-레벨 경영진 및 이사회 보안 자문 서비스
- 위험 정량화
- 인수합병 관련 보안 위험 평가
- 클라우드 보안 및 규제 준수
- 데이터 프라이버시 전략
- 규제 준수 및 거버넌스
- 서드파티 보안 위험 평가 및 관리
- 자동화된 IT 위험 관리
- 중요 인프라 보안
- SAP 보안 전략 평가 및 위험 감소
- 직원의 보안 인식 관리

SSRC는 보안 위험을 평가하고 감소시키고 관리하도록 지원합니다. 비즈니스에 규제 준수에 관한 전문가의 조언이 필요하건, 데이터 프라이버시 준비 상태를 검토하건, 리더십에 대한 위험을 정량화하건, IBM Security Strategy Risk and Compliance 서비스를 찾으십시오.

IBM Security Command Center: 최악의 상황에 대비하도록 지원하고 전반적인 보안 문화와 준비 태세를 향상하는 일은 IBM의 Command Center가 가장 잘 하는 일입니다. 사이버 레인지에 참여하면 여러 부서로 구성된 팀이 시뮬레이션된 보안 상황에 몰입함으로써 실제 환경에서 큰 대가를 초래하는 사이버 공격 상황에 대처하는 데 필요한 스킬과 자신감을 개발하고 연마할 수 있습니다. Executive Briefing Center에서는 보안 태세를 대폭 개선하고 위험에 대한 노출을 최소화하도록 돕는 숙련된 인시던트 대응 요원, 침투 테스트 수행자, 보안 전략가 및 리더 등 IBM의 보안 전문가들을 활용할 수 있습니다.

관련 주제

규제 준수: 조직은 데이터가 미사용 상태이건 이동 중인 상태이건 해당 데이터가 어떻게 처리되는지를 추적하여 어느 시점에서든 규제를 준수했음을 증명할 수 있어야 합니다. 관리하고 실행하기 쉬운 규제 준수 기능으로 규제 변화에 선제적으로 대응할 수 있습니다. 또한, 조직의 규제 준수 지원 솔루션을 사용하면 리소스를 다른 우선 과제에 활용할 수 있습니다. IBM Security의 인재와 기술을 활용하여 규제 준수를 간소화하십시오.

리더십 및 문화: 기술 혁신, 시장의 대대적인 변화, 스킬 요구사항의 변화, 그리고 기타 요인으로 인해 보안과 규제 준수 상태에 영향을 줄 수 있는 불안정성이 초래될 수 있습니다. 조직을 보호해주는 마법의 방패는 없지만 보안 트렌드와 혁신적인 솔루션에 관한 최신 연구와 인사이트를 활용하면 보안 및 규제 준수 상태 개선을 위한 효과적인 조치를 취할 수 있습니다.

## 출처

1. Ponemon Institute 및 IBM Security, “2019 Cost of a Data Breach Report”, 2019.

IBM Security


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

Produced in the United States of America
2020년 1월


GDPYL8KD