Gartner

2023 리더십 비전

보안/리스크 관리 리더를 위한 톱3 전략적 우선순위

Tom Scholtz(Distinguished VP Analyst)

지금의 기업들은 계속적 고물가, 귀하고 비싼 인재, 러시아의 우크라이나 침공으로 인한 글로벌 공급망 장애, 코로나19 봉쇄, 에너지 부족 등으로 인해 발생한 불확실성에 직면하고 있다. 이러한 삼중고는 2023년 전세계 비즈니스와 사이버보안/위협 환경에 직접적인 영향을 미치고 있다.

지금과 같은 어려운 시기에 사이버보안 리더가 내리는 의사결정은 조직이 불필요한 사이버보안 리스크를 감수할 것인지, 아니면 기술 혁신을 활용하여 성공으로 나아갈 수 있을 것인지를 결정한다. 사이버보안 팀은 민첩하게 전환할 수 있어야 한다.

2023년으로 이어지는 경제적 불확실성과 여러 장애요소들에도 불구하고, 정보 보안 담당 임원(CISO)은 사이버보안에 계속적으로 투자할 계획을 유지하고 있다. 사이버보안 리스크는 기술 의사결정권이 분산되면서 더욱 증가하고 있다. 높은 성과를 내는 CISO는 새로운 아이디어들을 실험할 용기를 가지고 있다. 그들은 리더로서의 효과성을 높이고, 조직 내 문화 변화를 주도하는데 초점을 맞추고, 사이버 판단의 도입을 지지해야 한다.

기업이 경쟁자들로부터 자신을 차별화하고 혁신하기 위해 계속적으로 기술에 투자함에 따라, 보안/리스크 관리(SRM) 리더는 리스크를 판단/관리하고, 보안 모범 관행들에 대해 자신이 속한 조직을 교육시키고 이끄는 새로운 방법들을 실행해야 한다.

가트너 리더십 비전은 데이터 지향 리서치를 기반으로 해당 영역 리더와 팀이 어디에 초점을 맞추어야 하는 지에 대한 최고 수준의 가이드를 제공한다. 가트너는 여러 직무들을 아우르는 고객들에게 상세한 인사이트를 제공하고, 이제는 비즈니스 커뮤니티 전체에 그 내용의 일부를 공유하고자 한다. 우리는 이것이 당신의 팀, 동료, 다른 리더들과의 논의에 초점을 제공하고, 2023년의 전략적 계획들을 구체화할 때 우선순위와 행동들을 보다 빠르고 효과적으로 정리하는데 도움이 되기를 바란다.

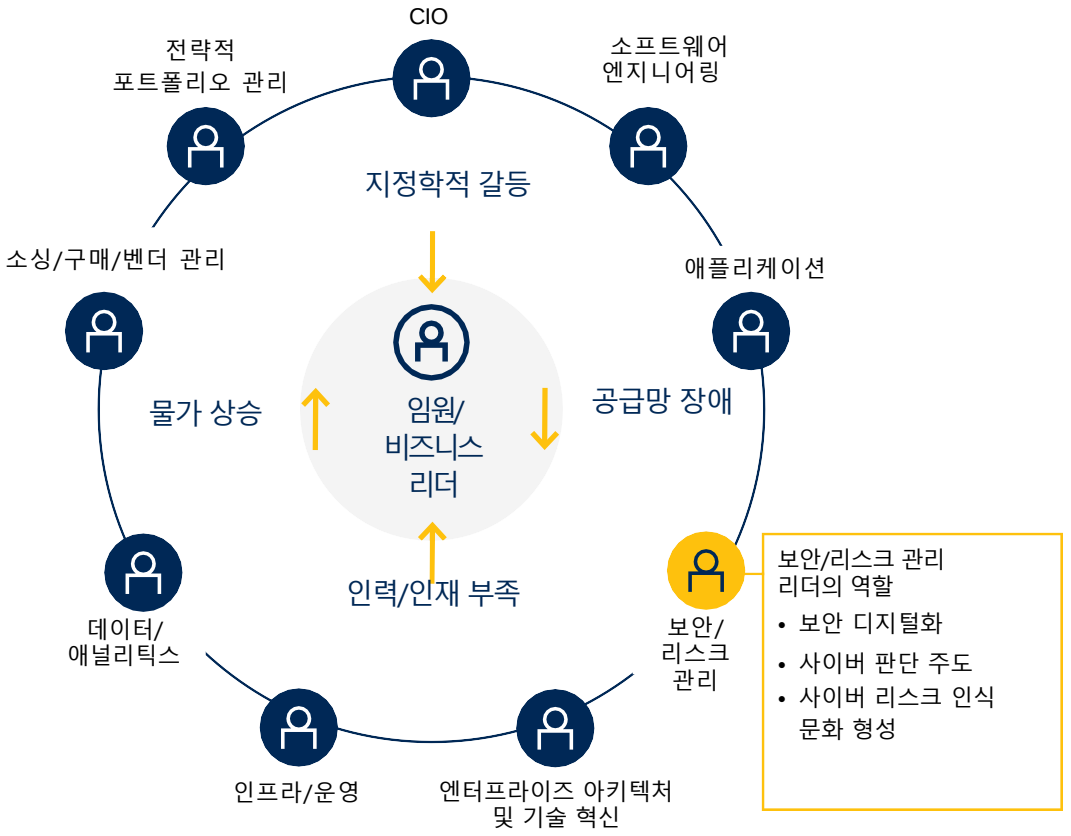
Tom Scholtz
Distinguished VP Analyst

독특한 비즈니스 환경은 팀 노력을 요구한다

보안/리스크 관리 리더는 갈수록 복잡하고 위험해지는 환경에서 보안 디지털화를 실현하기 위해 노력한다.

기업들은 경쟁 차별화를 위한 혁신 기술들을 탐색하면서 불확실한 비즈니스 환경에 대처해나가야 하는 상황에 있고, 이 때문에 리스크 수용도를 높이고 가까운 미래에 대한 보안에 많은 투자를 하고자 한다.

내외부 도전들을 이해하고 대응하기 위해, 보안/리스크 관리 리더는 비즈니스 리더들이 정보에 기반한 높은 수준의 보안 리스크 관련 의사결정을 내릴 수 있는 지식과 역량을 갖추게 하는 동시에 조직 전반에 포진한 이해관계자들과 협업해야 한다.



출처: Gartner

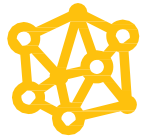
보안/리스크 관리 리더에 영향을 주는 핵심 동향 3가지

IT 조직 밖에서 일하는 기술 전문가 증가

디지털 가속화를 보다 효과적으로 실현하기 위해, 67%의 CEO들이 보다 많은 기술 업무가 비즈니스 영역에서 수행되기를 원한다. 이는 보안/리스크 관리 리더의 직접 통제 밖에 있는 팀들에 '비즈니스 기술 전문가'들이 늘어난다는 의미이다. 이들은 기술을 활용할 뿐만 아니라 만들어 낼 수도 있는 IT 조직 밖에서 일하는 직원들이다.

제삼자 보안 리스크 증가

최근의 사이버보안 사건/사고들은 공급망 내 취약성을 드러내었다. 2025년까지, 60%의 조직들이 정보, 시스템, 인프라 관련 피해를 방지하기 위해 제삼자 거래를 하는 데 있어 사이버보안 리스크를 중요 요소로 활용할 것이다.



사이버보안 메시**(mesh)** 진화

엔드포인트, 디지털 시민, IT 자산이 어디에든 위치할 수 있다면, 사이버보안 통제도 마찬가지가 되어야 한다. 사이버보안 메시는 조합형 분산 도구 및 통제로 이루어진 고도로 유연하고 협업적 생태계로서 전세계 여러 조직들의 자산을 보호하기 위해 성공적으로 적용되고 있다.

보안/리스크 관리 리더의 도전 및 행동

1 사람 요소 다루기

대부분은 데이터 유출 사고/사건은 여전히 사람 요소와 연관된다. 최근 가트너 조사에 의하면, 직원들은 여러 계정에 대해 같은 비밀번호를 사용하거나 업무 기기에서 알려지지 않은 출처로부터의 이메일을 여는 등 이미 인식된 보안 리스크가 있는 행동을 (때로는 알면서도) 하고 있다.

2 보안/리스크 관리 효과성 향상

현재 이해관계자의 기대를 넘어서는 성과를 내는 보안/리스크 관리 리더는 12%에 불과하다.. 리더들은 각자의 모든 책임 영역들에 대한 효과성을 향상시켜 사이버보안 우선순위 성과를 낼 수 있는 능력을 보여야 한다.

3 사이버 판단 여정 가속화

보안/리스크 관리 리더들은 전사적으로 이해관계자들을 지원하여 보안/리스크 관리 팀이나 자동화에 의존하기 보다 독립적으로 정보에 기반한 리스크 관련 의사결정(사이버 판단)을 내릴 수 있게 해야 한다.

보안/리스크 관리 리더의 행동

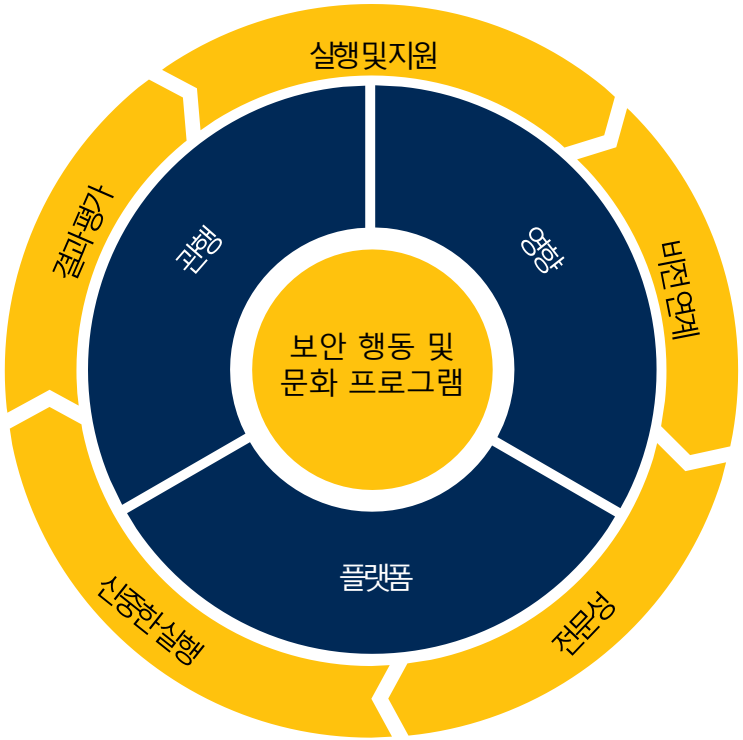
관행, 영향, 플랫폼, 동인 등에 초점을 맞추는 가트너 PIPE 프레임워크를 활용하여 보안 행동 및 문화 프로그램의 성공적 실행을 위한 지침을 제공한다.

파악된 범주들에 대한 효과성을 향상시키는데 초점을 맞추어 비즈니스 우선순위들과 더 잘 정렬될 수 있게 하고 조직을 보호해야 한다.

자가 인증, 그룹 신뢰 점수 등의 전략을 통해 자율성을 지원하여 전사적으로 사이버 판단 능력을 강화하도록 한다.

보안 리스크 관련 사람 요소를 줄인다

사이버보안 리스크에 대한 사람 행동의 부정적 파급효과를 감소시키기 위해, 보안/리스크 관리 리더는 보안 훈련 프로그램에 대해 이전과는 획기적으로 다른 접근법을 취해야 한다. 가트너 PIPE 프레임워크가 이에 대한 방향을 제시할 수 있다. 리더는 제삼자와의 상호작용에 대한 모범 관행을 정립하여 디지털 공급망 리스크도 관리하여야 한다.



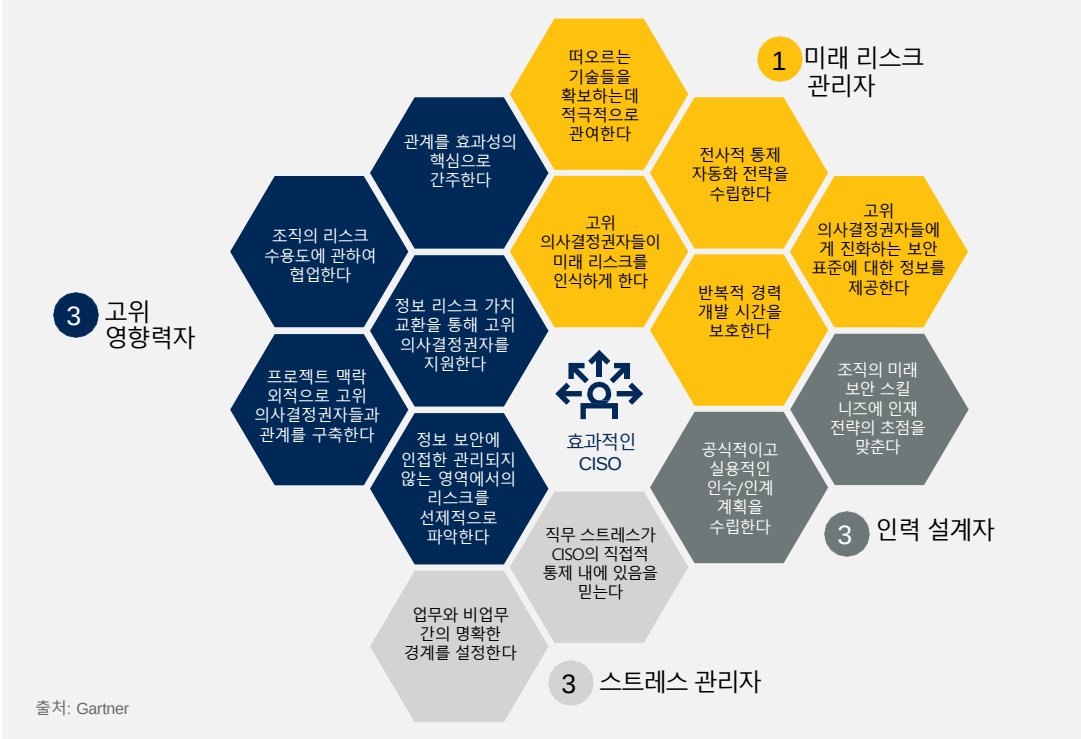
출처: Gartner

다음 단계에 대한 조언

1. 통제 체계를 설계할 때 사용자 경험을 고려한다.
2. 직무 관련 사이버보안 학습 경험을 설계한다.
3. 결과물 지향 지표에 초점을 맞추어 조직이 얼마나 잘 보호되는지를 판단한다.
4. 공급망 벤더들과 연계할 때,
   - 공유된 데이터 및 인프라 전반에 대한 잠재적 보안 리스크를 파악한다.
   - 새로운 규제 사항들을 준수한다.
   - 이해관계자들과 핵심 파트너십을 구축하여 공동 거버넌스를 개발한다.
   - 떠오르는 모범 관행들을 평가, 실행한다.

리더십 효과성을 향상시킨다

보안/리스크 관리 리더의 역할이 계속적으로 진화, 확장됨에 따라, 해당 범주들에 대한 리더십 효과성을 지속적으로 평가하고 향상시키는 것이 중요하다. 보안/리스크 관리 리더는 자신의 우선순위 이슈들을 비즈니스 우선순위 이슈들과 정렬시켜 가치 창출을 촉진함과 동시에 조직을 보호해야 한다.



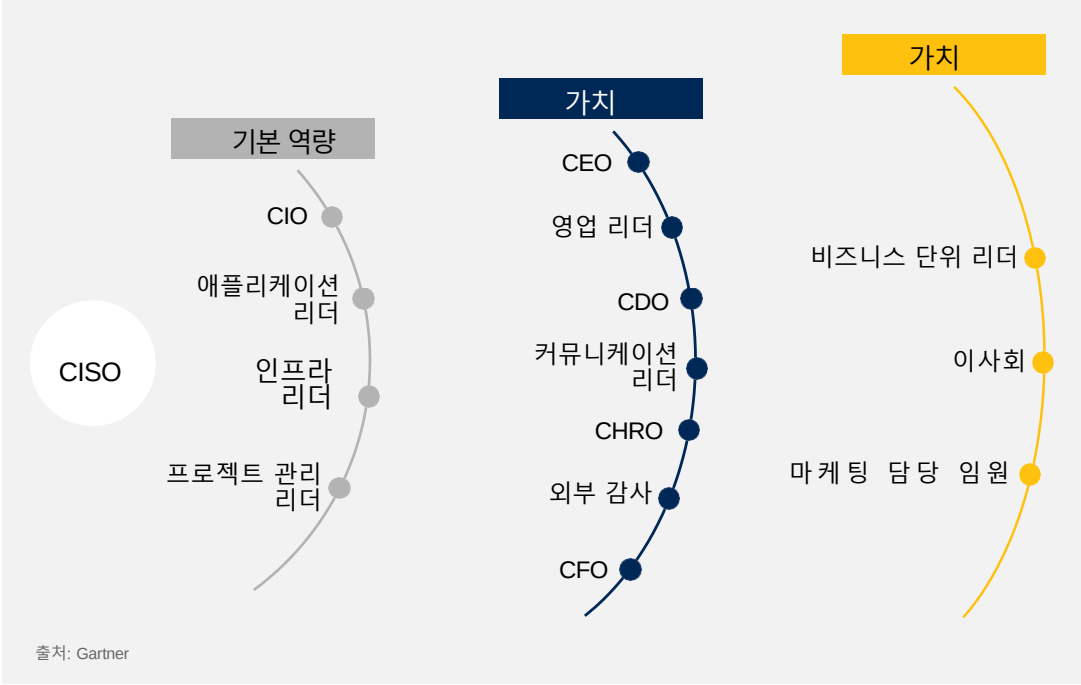
출처: Gartner

다음 단계 조언

1. IT 영역 밖의 고위 의사결정권자들과 관계를 구축한다.
2. 의사결정권자들에게 새로운 보안 표준에 대한 정보를 제공하여 미래 리스크에 대비한다.
3. 인공지능의 비즈니스 활용에 대한 보안을 선제적으로 준비한다.
4. 인력 성과를 추적하고 역량 격차 문제를 창의적으로 해결한다.
5. 업무와 개인 삶 간의 경계를 유지하여 스트레스를 관리하다.

전사적 보안 역량을 강화한다

보안/리스크 관리 리더의 직접적 영향력 밖에 있는 그룹들이 사이버보안 활동을 독자적으로 수행할 수 있도록 지원함으로써 전사적 경쟁력을 개발하고 보안/리스크 관리 팀이 보다 부가가치가 큰 활동들에 초점을 맞출 수 있다. 사이버보안 메시 전략을 수립, 실행하는 것은 자산이 어디에 위치하든 통합된 시스템의 보안을 강화하고 접근, 설정, 데이터를 보호하는데 도움을 준다.



출처: Gartner

다음 단계 조언

1. 딜리버리 팀이 QP Express 프로그램을 통해 출시 예정 애플리케이션들을 자가 인증할 수 있도록 권한을 부여한다.
2. 그룹 신뢰 점수를 활용하여 사이버보안 활동을 수행할 수 있는 팀들을 파악한다.
3. 사이버보안 메시 전략을 수립, 실행한다.
   - 현재 활용 중인 도구들의 성숙도를 평가한다.
   - 팀의 통합 능력을 조사한다.
   - 적정 투자 수준을 결정한다.
   - 고유 통합 및 개방 표준을 혼합하여 통합 플랫폼, 계층화된 조합형 제품 혹은 결합된 접근을 어떻게 구축할 것인지를 정한다.

실용적, 객관적 인사이트

보안 리더를 위한 추가적 자료 및 도구

도구

IT Score for Security and Risk Management

최우선순위 활동들에 대한 관점 확보하기

자세히 알아보기

로드맵

The IT Roadmap for Cybersecurity

탄력, 확장성, 민첩성을 갖춘 사이버보안 전략 수립하기

다운로드 하기

전자책

3 Must-Haves in Your Cybersecurity Incident Response Plan

사이버보안 사건/사고에 대한 조직의 대응 능력 강화하기

다운로드 하기

전자책

Four Facets of Effective CISO Leadership

상위 성과 리더들이 그들의 확장하는 담당 영역을 어떻게 관리하는지 파악하기

다운로드 하기

이미 가트너 고객사라면,
고객사 포털을 통해 더 많은 자료를 확인하실 수 있습니다. 로그인

Gartner

가트너 컨퍼런스에 참석하여 **2023**년 **IT** 전략을 강화하십시오!

2022년, 가트너는 34건의 컨퍼런스를 개최하였고 여기에 46,000명 이상의 비즈니스 및 기술 전문가들이 참석하였습니다. 학습을 가속화하고, 의사결정에 방향성을 부여하고, 중요 동향을 파악할 수 있는 올해의 가트너 컨퍼런스에 참석하시어 다른 전향적 사고 리더들과 교류하시기 바랍니다.

놓치지 마십시오.

지금 2023년 컨퍼런스 달력을 확인하시고 자신에게 적합한 컨퍼런스를 찾으십시오.

→ 컨퍼런스 달력 확인하기








가트너 고객사가 되십시오

가트너는 귀사의 최우선순위 이슈들에 대한 실용적이고 객관적인 인사이트를 제공합니다. 가트너의 전문가 조언과 도구는 보다 빠르고 스마트한 의사결정과 향상된 성과 창출을 가능하게 합니다. 아래 연락처를 통해 가트너 고객사가 되실 수 있습니다.

미국: 1866 263 8917

미국 외: +44 (0) 03301 628 476

가트너 고객사 되기

IT 리더를 위한 가트너 서비스에 대해 자세히 알아보기

gartner.com/en/cybersecurity

소셜미디어로 가트너 인사이트 얻기

Gartner