데이터 중심 보안의 실태

Informatica 후원

Ponemon Institute LLC에서 독립적으로 수행

발행일: 2014년 6월

데이터 중심 보안의 실태

Ponemon Institute, 2014년 6월

1부. 머리말

Ponemon Institute에서 Informatica의 후원으로 실시한 *데이터 중심 보안의 실태*에 대한 조사 결과를 발표하겠습니다. 본 조사의 목적은 조직에서 정형 및 비정형 데이터의 보안 위협에 어떻게 대처하고 있는지를 파악하는 것입니다. 결과에 따르면, 민감하고 기밀인 데이터의 위치에 대한 불확실성이 해커나 악의적인 직원보다 더 우려되는 상황이었습니다.

이 설문 조사는 전세계 16개국의 글로벌 IT 및 IT 보안 실무자 1,587명을 대상으로 실시되었습니다.[1] 참여 국가 목록은 이 보고서의 부록에 수록되어 있습니다. 지식을 바탕으로 한 수준 높은 대답을 얻기 위해 민감하거나 기밀인 정형 및 비정형 데이터의 보호와 관련 있는 직무에 종사하는 IT 실무자만을 대상으로 했습니다.

데이터 중심 보안은 데이터가 생성될 때 데이터 보안 정책을 할당하고, 기술 플랫폼, 지역 또는 호스팅 플랫폼에 상관없이 데이터가 복제, 복사 또는 통합되는 곳마다 데이터에 적용됩니다. 데이터 중심 보안은 데이터 마스킹, 암호화, 토큰화 및 데이터베이스 활동 모니터링과 같은 기술을 포함합니다. 그러나 본 조사에서는 자동화된 솔루션이 조직의 규정 준수 및 데이터 보호 전략을 개선하는 데 도움이 되는 것으로 나타났습니다.

본 조사의 주요 결과

- **데이터의 위치를 모르기 때문에 IT 실무자가 야근 근무를 해야 하는 것으로 나타났습니다.** 응답자의 57%가 조직의 민감하거나 기밀인 데이터가 있는 곳을 모르기 때문에 야간 근무를 해야 한다고 응답했습니다. 그 다음으로는 51%가 새로운 모바일 플랫폼으로 마이그레이션이 우려 사항이라고 응답했습니다.

- **민감하거나 기밀인 데이터가 IT 보안에 포착되지 않는 경우가 많았습니다.** 응답자의 16%만 민감한 정형 데이터가 있는 곳을 모두 알고 있다고 생각했으며, 비정형 데이터가 상주하는 곳을 알고 있다는 응답자는 극소수(7%)에 불과했습니다.

- **조직에서는 데이터 자산을 보호하기 위해 주로 민감한 데이터의 분류에 의존했습니다.** 정형 데이터에 가장 일반적으로 사용되는 두 가지 기술은 민감한 데이터 분류와 애플리케이션 수준의 액세스 제어였습니다. 19%만 조직에서 중앙 집중식 액세스 제어 관리 및 권한 부여를 사용한다고 응답했으며, 파일 시스템 및 액세스 감사를 사용하는 응답자는 14%에 불과했습니다.

- **자동화된 민감한 데이터 검색 솔루션이 데이터에 대한 위험을 줄이고 보안 효과를 증대시킨다고 믿는 것으로 나타났습니다.** 자동화된 솔루션에 대한 긍정적인 인식에도 불구하고 응답자의 60%는 민감하거나 기밀인 데이터가 있는 곳을 검색하기 위해 자동화된 솔루션을 사용하고 있지 않다고 응답했습니다. 해당 조직에서 자동화된 솔루션을 사용한다는 40%의 응답자 중 64%는 데이터베이스 및 엔터프라이즈 애플리케이션에서 민감하거나 기밀인 데이터가 있는 곳을 검색하는 데 자동화된 솔루션을 사용한다고 응답했습니다. 파일 및 전자 메일에서 데이터를 검색하는 데 자동화된 솔루션을 사용하는 응답자는 22%에 불과했습니다.

[1] 이 글로벌 표본을 북미, 유럽 및 기타 국가의 3개 지역에 따라 분석했습니다.

- **전문 자동화된 솔루션이 조직의 규정 준수 및 데이터 보호 전략을 개선하는 데 도움이 된다고 생각하는 것으로 나타났습니다.** 가장 일반적으로 사용되는 기능은 실시간 모니터링을 통한 자동화된 사용자 액세스 기록이었으며, 그 다음은 정책 워크플로우 자동화였습니다.

2부. 주요 결과

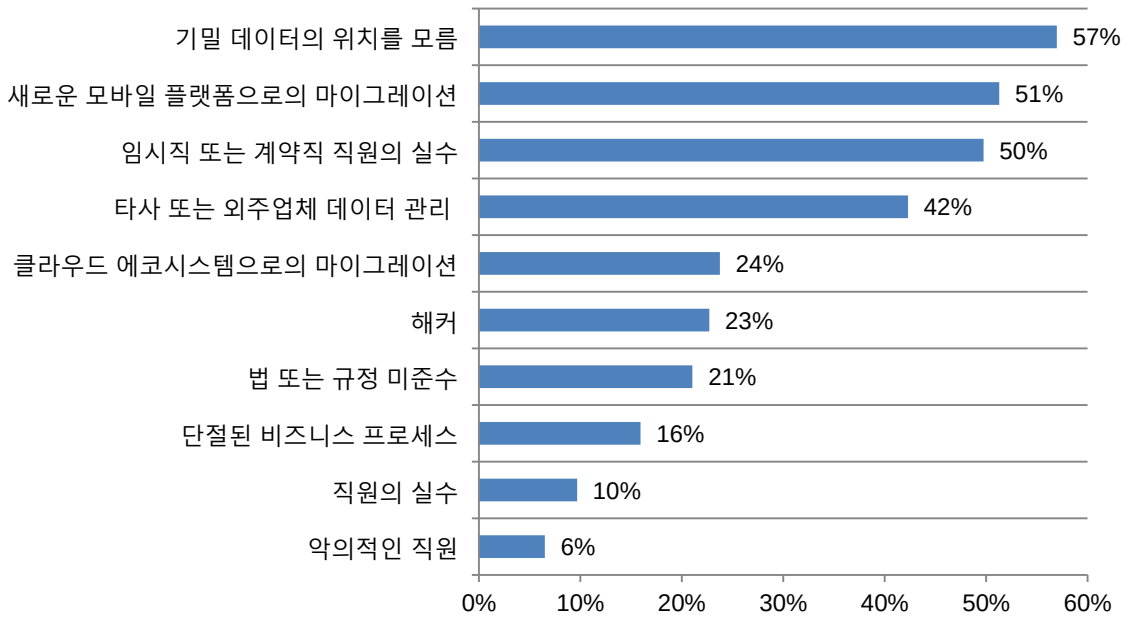
이 섹션에서는 종합적인 결과에 대한 분석을 제공합니다. 감사된 전체 결과는 이 보고서의 부록에 수록되어 있습니다. 이 보고서는 다음 주제에 따라 구성되었습니다.

- 데이터의 위치를 모르기 때문에 IT 실무자가 야간 근무를 해야 함
- 보안 솔루션이 데이터의 위치 및 사용자 액세스에 대한 가시성을 향상시키지 않는 경우가 많음
- 적합한 솔루션이 있다면 안심할 수 있음

데이터의 위치를 모르기 때문에 IT 실무자가 야간 근무를 해야 함

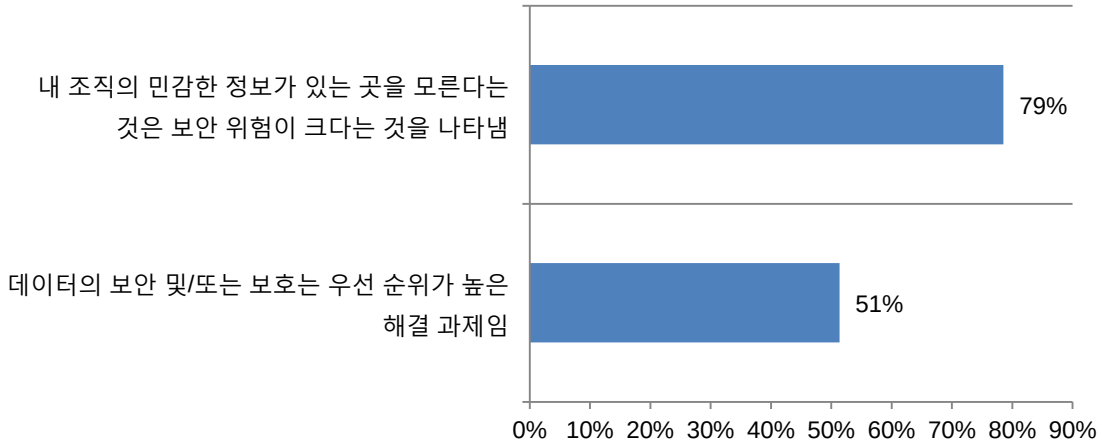
민감하거나 기밀인 데이터의 위치를 모르기 때문에 대부분의 응답자가 야간 근무를 해야 하며, 이는 보안 위험이 크다는 것을 나타냅니다. 응답자에게 IT 보안 실무자를 곤혹스럽게 만들 수 있는 위협 및 위험 목록을 제시했습니다. 그림 1에서는 응답자의 57%가 조직의 민감하거나 기밀인 데이터가 있는 곳을 모르기 때문에 야간 근무를 해야 한다고 응답한 것을 보여 줍니다. 그 다음으로는 51%가 새로운 모바일 플랫폼으로 마이그레이션이 우려 사항이라고 응답했습니다. 해커, 규정 미준수 및 악의적인 직원은 목록에서 하위에 위치해 있습니다.

그림 1. 야간 근무를 해야 하는 이유는 무엇입니까?
(최대 3개 선택)



데이터 보안은 심각한 위협이지만 우선 과제가 아닌 경우가 많았습니다. 그림 2에서는 민감하고 기밀인 정보가 상주하는 곳을 모른다는 것이 심각한 위협이라는 점에 동의하는 응답자의 비율과 이것이 해당 조직에서 우선 순위가 높은 해결 과제라고 생각하는 응답자의 비율 간에 상당한 격차가 있음을 보여 줍니다. 응답자의 79%는 이것이 해당 조직에서 직면한 상당한 보안 위험이라는 데 동의했지만 데이터 보안 및/또는 보호가 해당 조직에서 우선 순위가 높은 해결 과제라고 생각하는 응답자의 비율(51%)은 그보다 훨씬 적었습니다. 이 차이는 위험을 완화하는 데 필요한 리소스를 확보하는 데 어려움이 있을 수 있음을 나타냅니다.

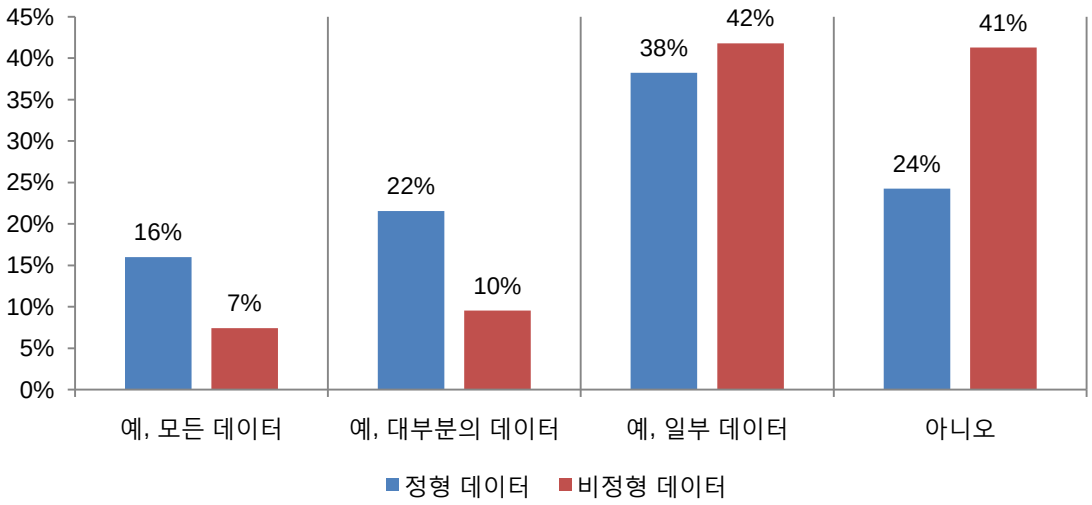
그림 2. 민감한 데이터의 보안에 대한 개인적인 의견
(매우 그렇다 + 그렇다)



대부분의 조직이 민감하거나 기밀인 데이터가 있는 곳을 모르고 있습니다. 그림 3을 보면, 응답자의 16%만 민감한 정형 데이터가 있는 곳을 모두 알고 있다고 생각했으며, 비정형 데이터가 상주하는 곳을 알고 있다는 응답자는 극소수(7%)에 불과한 것을 알 수 있습니다.

정형 및 비정형 데이터의 위치를 알고 있는지에 관한 응답에도 큰 차이가 있었습니다. 정형 데이터의 위치를 모르는 응답자는 24%인 반면, 조직의 비정형 데이터를 파악하지 못하는 응답자는 41%였습니다.

그림 3. 민감하거나 기밀인 데이터가 있는 곳을 아십니까?

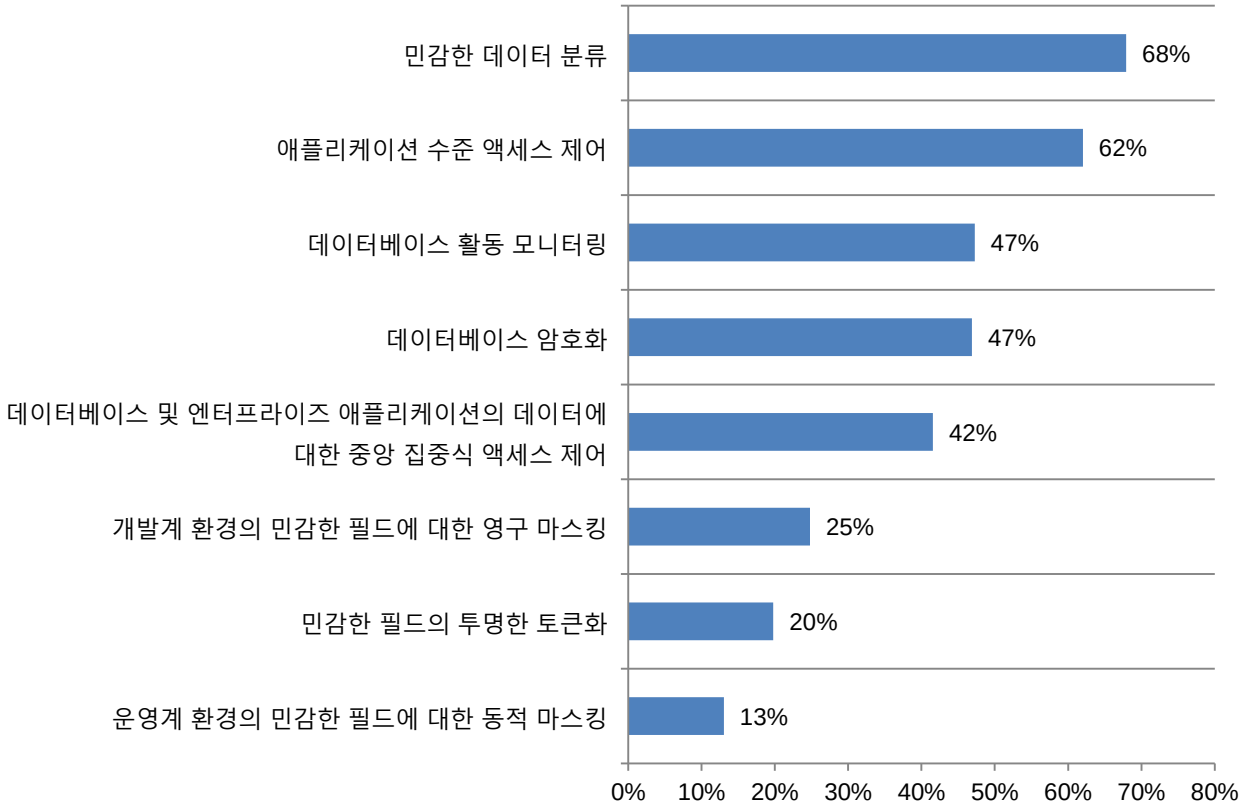


보안 솔루션이 데이터의 위치 및 사용자 액세스에 대한 가시성을 향상시키지 않는 경우가 많음

조직에서는 정형 및 비정형 데이터 자산을 보호하기 위해 주로 민감한 데이터의 분류에 의존했습니다. 응답자들은 정형 데이터와 비정형 데이터를 모두 포함하여 해당 조직에 있는 데이터의 평균 34%만 민감하거나 기밀인 것으로 분류할 수 있는 것으로 추정했습니다. 응답자의 53%가 고객 데이터를 가장 위험한 것으로 간주했으며, 그 다음으로 38%가 지적 재산이라고 응답했습니다.

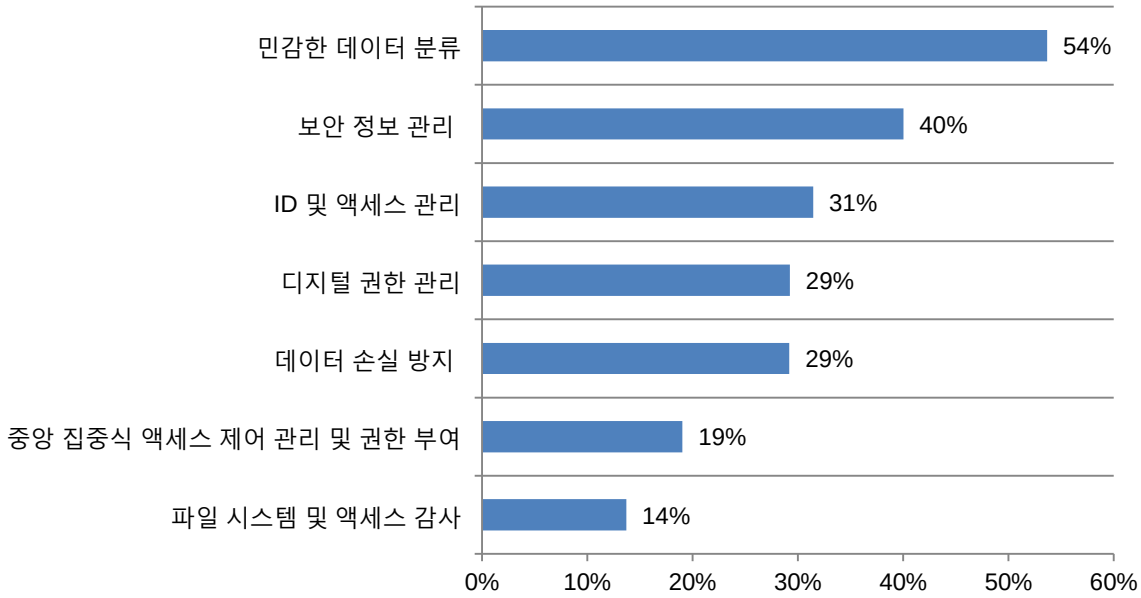
그림 4에서는 조직에서 정형 데이터 자산을 보호하기 위해 사용하고 있는 기술이나 툴을 보여줍니다. 정형 데이터에 가장 일반적으로 사용되는 두 가지는 민감한 데이터 분류와 애플리케이션 수준의 액세스 제어였습니다.

그림 4. 정형 데이터 자산을 보호하기 위한 기술
(2개 이상 선택 가능)



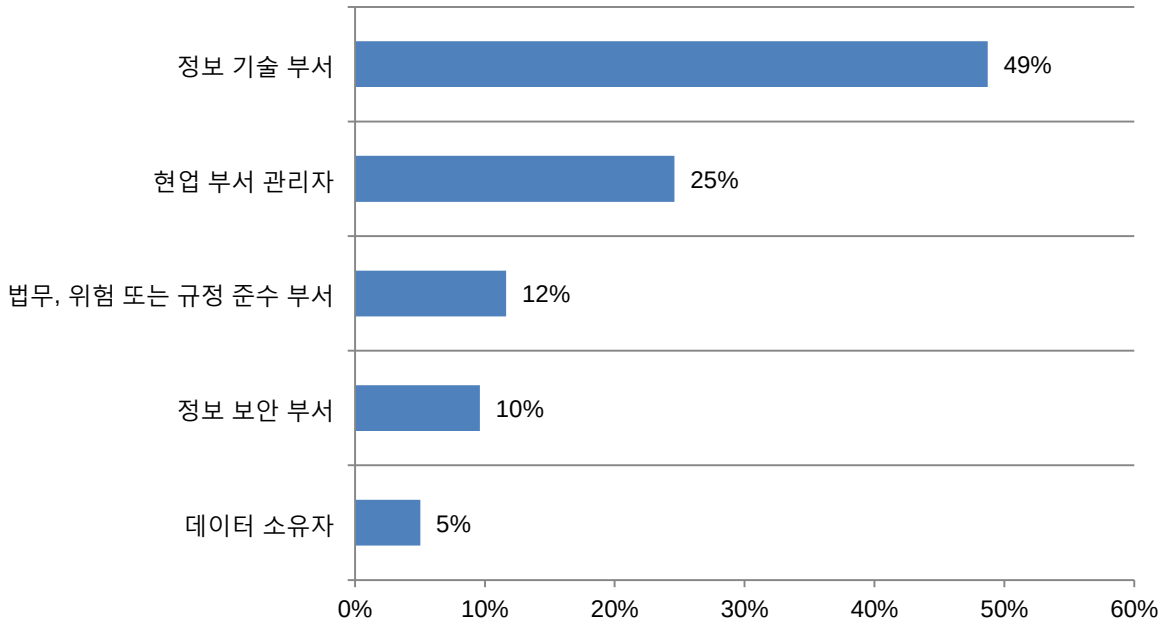
비정형 데이터의 경우(그림 5), 민감한 데이터 분류를 가장 많이 사용하고, 그 다음으로 보안 정보 관리 시스템을 많이 사용하고 있었습니다.

그림 5. 비정형 데이터 자산을 보호하기 위한 기술
(2개 이상 선택 가능)



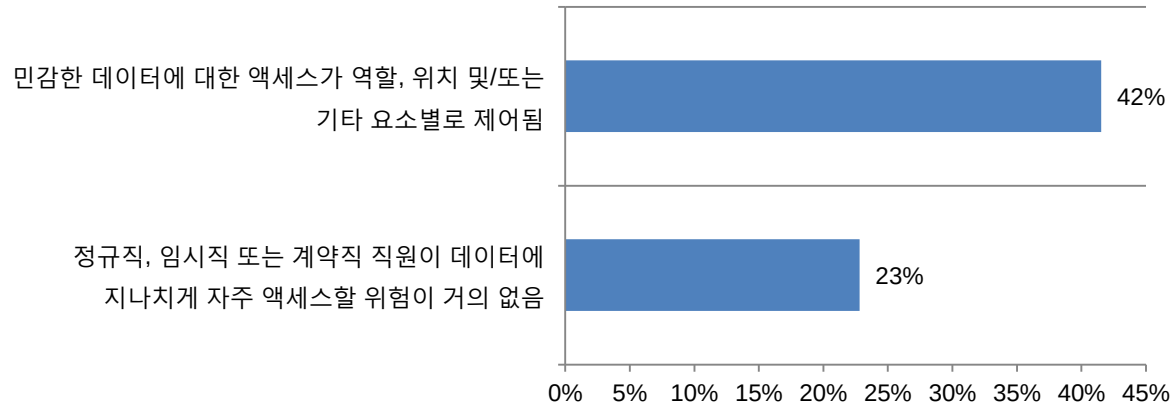
사용자에게 데이터 자산에 대한 액세스 권한을 부여하는 책임은 주로 IT 부서에 있었습니다. 그림 6을 보면, 49%가 IT 부서에서 직원들에게 액세스 권한을 부여한다고 응답했으며, 그 다음으로 25%가 현업 부서 관리자가 담당하고 있다고 응답했습니다.

그림 6. 사용자에게 데이터 자산에 대한 액세스 권한을 부여하는 책임은 누구에게 있습니까?
(최대 2개 선택)



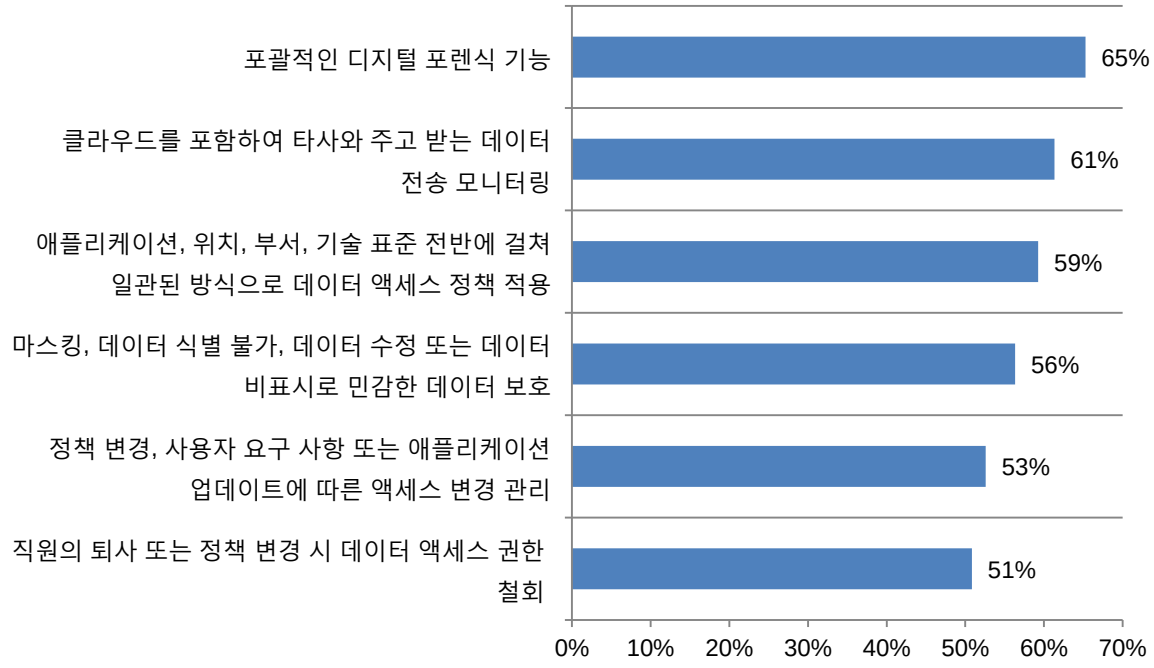
민감한 정보에 대한 액세스를 제어하는 것이 위험을 줄이는 데 매우 중요하다고 생각하는 것으로 나타났습니다. 그림 7에 나와 있듯이, 응답자의 42%가 민감한 데이터에 대한 액세스를 역할, 위치 및 기타 요소별로 제어하고 있다고 응답했습니다. 그러나 기업의 액세스 제어 절차는 성공적이지 못한 것으로 나타났습니다. 23%만이 정규직, 임시직 또는 계약직 직원에게 적절한 수준의 액세스 권한이 있으며, 이러한 개인이 지나치게 자주 액세스할 위험이 거의 없다고 생각했습니다.

그림 7. 민감한 데이터의 보안에 대한 개인적인 의견
(매우 그렇다 + 그렇다)



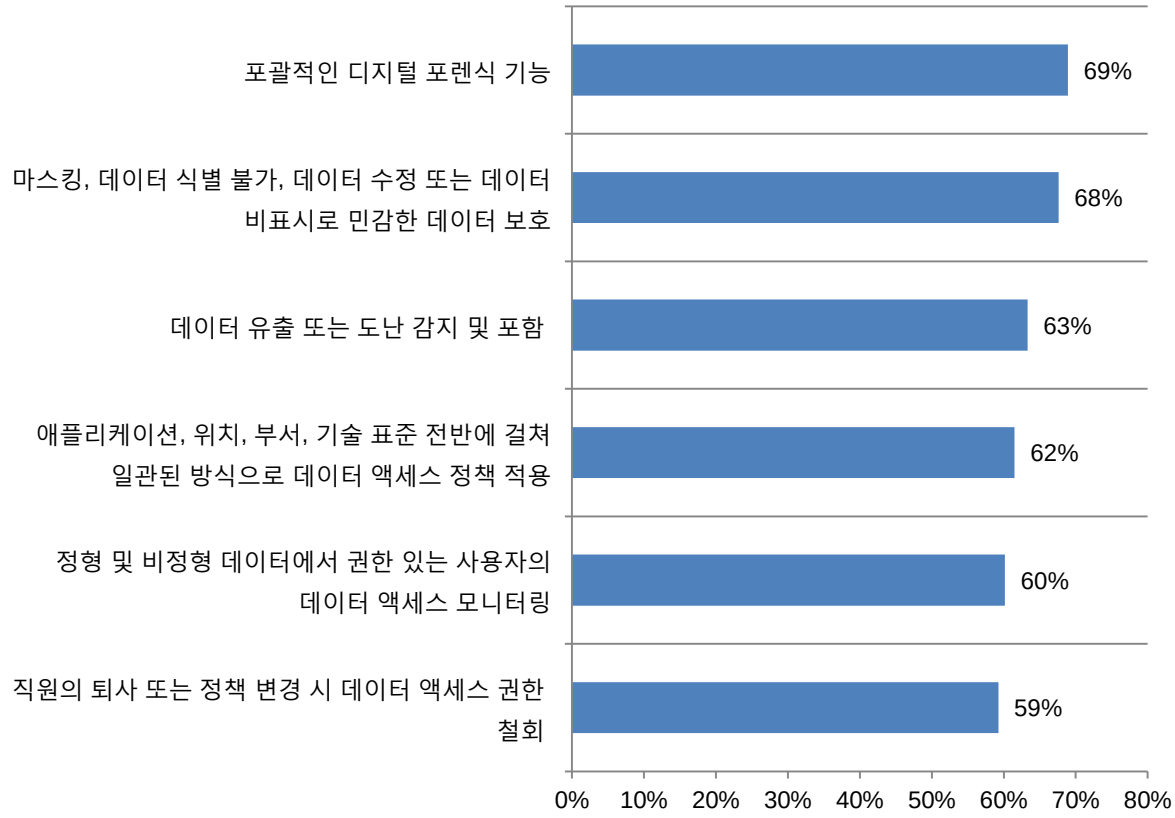
데이터 자산 보안 절차가 잘 이행되지 않거나 수립되어 있지 않은 것으로 나타났습니다. 그림 8에는 조직에 수립되어 있지 않은 보안 절차가 나와 있습니다. 그림을 보면, 대부분의 조직에서 포괄적인 디지털 포렌식을 사용하지 않고, 클라우드를 포함하여 타사와 주고 받는 데이터 전송 모니터링 및 일관된 방식으로 데이터 액세스 정책 적용을 사용하고 있지 않는 것을 알 수 있습니다.

그림 8. 데이터베이스의 데이터 자산에 대한 보안 절차
(절차가 잘 이행되지 않거나 수립되어 있지 않음)



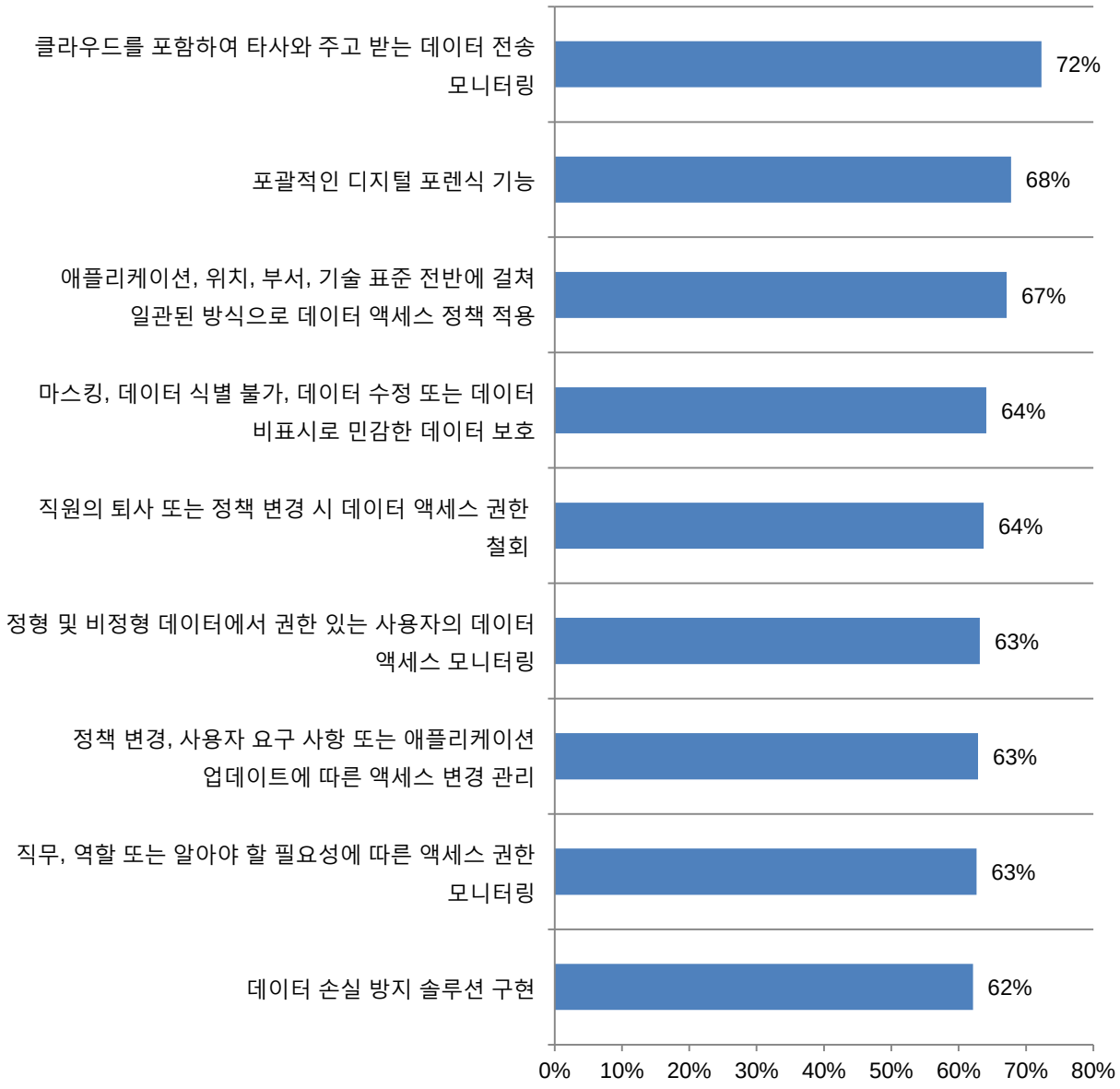
전자 메일 내 민감하고 기밀인 데이터에 대한 보안 절차가 대부분 수립되어 있지 않는 것으로 나타났습니다. 그림 9에서는 대다수의 조직이 포괄적인 디지털 포렌식을 사용하지 않고, 마스킹, 데이터 식별 불가, 데이터 수정 또는 데이터 비표시로 민감한 데이터를 보호하지 않으며, 애플리케이션, 위치, 부서 및 기술 표준 전반에 걸쳐 일관된 방식으로 데이터 액세스 정책을 적용하지 않고 있는 것을 보여 줍니다.

그림 9. 전자 메일의 데이터 자산에 대한 보안 절차
(절차가 잘 이행되지 않거나 수립되어 있지 않음)



파일 수준의 데이터 보안 절차에서는 클라우드를 포함하여 타사와 주고 받는 데이터 전송을 모니터링하지 않는 경우가 많은 것으로 나타났습니다. 그림 10에서는 파일의 데이터 자산에 대한 보안 절차가 해당 조직에서 잘 이행되지 않거나 수립되어 있지 않은 것으로 응답한 결과를 보여 줍니다. 데이터 전송을 모니터링하지 않을 뿐 아니라 포괄적인 데이터 포렌식 기능이 없거나 애플리케이션 및 위치 간에 일관된 방식으로 데이터 액세스 정책을 적용하지도 않는 것으로 나타났습니다.

그림 10. 파일의 데이터 자산에 대한 보안 절차
(절차가 잘 이행되지 않거나 수립되어 있지 않음)

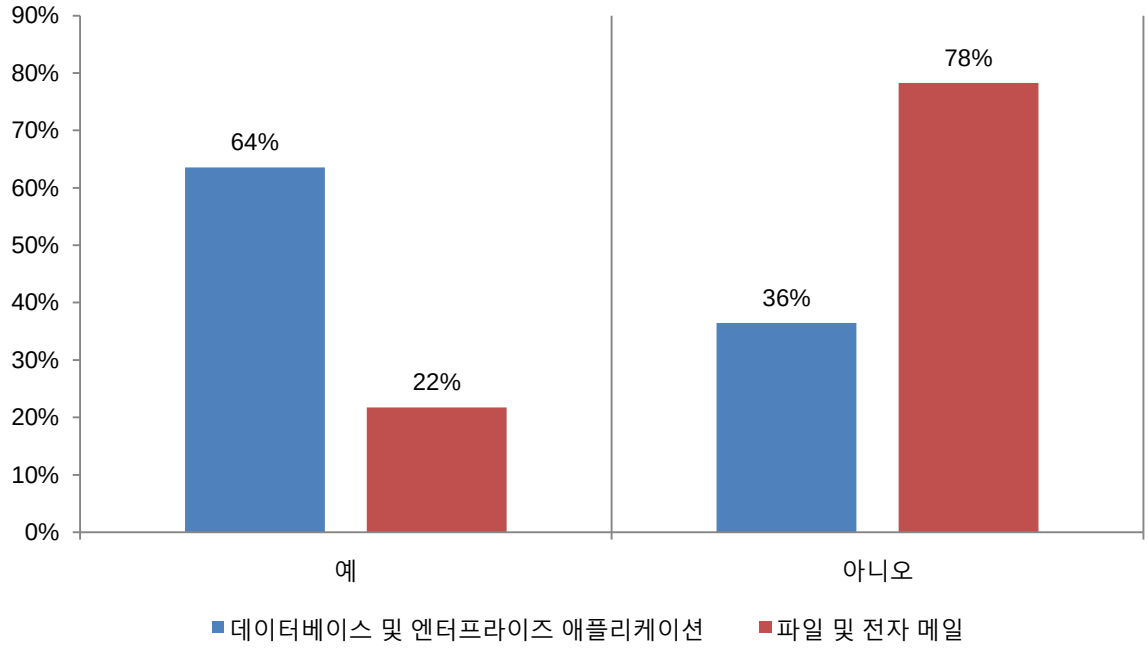


적합한 솔루션이 있다면 안심할 수 있음

자동화된 민감한 데이터 검색 솔루션이 데이터에 대한 위험을 줄이고 보안 효과를 증대시킨다고 믿는 것으로 나타났습니다. 자동화된 솔루션에 대한 긍정적인 인식에도 불구하고 응답자의 60%는 민감하거나 기밀인 데이터가 있는 곳을 검색하기 위해 자동화된 솔루션을 사용하고 있지 않다고 응답했습니다.

그림 11에서 보듯이 해당 조직에서 자동화된 솔루션을 사용한다는 40%의 응답자 중 64%는 데이터베이스 및 엔터프라이즈 애플리케이션에서 민감하거나 기밀인 데이터가 있는 곳을 검색하는 데 자동화된 솔루션을 사용한다고 응답했습니다. 파일 및 전자 메일에서 이러한 데이터가 있는 곳을 검색하기 위한 자동화된 솔루션이 있다고 응답한 응답자는 22%에 불과했습니다.

그림 11. 데이터베이스, 엔터프라이즈 애플리케이션, 파일 및 전자 메일에서 민감하거나 기밀인 데이터를 검색하는 데 자동화된 솔루션 사용

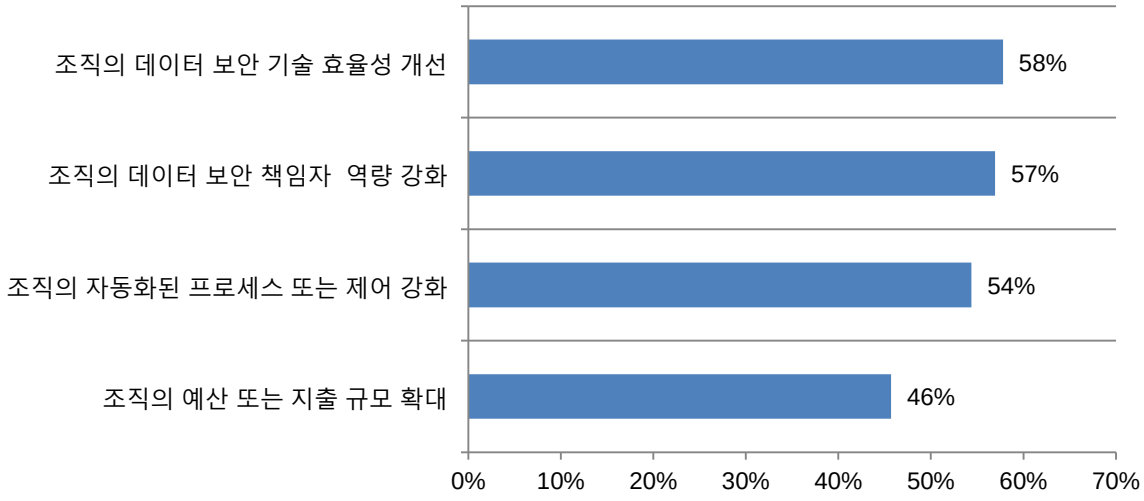


데이터 규정 위반이 감소할 수 있습니다. 본 조사에 참여한 조직의 72%가 지난 12개월 동안 데이터 규정 위반을 경험한 것으로 나타났습니다. 응답자들은 효과적인 데이터 보안 기술 및 숙련된 직원을 통해 데이터 규정 위반 사고를 방지할 수 있다고 응답했습니다.

데이터 규정 위반을 방지하거나 규모 및 빈도를 줄일 수 있는 방법은 그림 12에 나와 있습니다. 58%의 응답자가 보다 효과적인 데이터 보안 기술로 위험을 줄일 수 있다고 응답했으며, 57%는 보다 숙련된 데이터 보안 담당자가 데이터 규정 위반 가능성을 줄일 수 있다고 응답했습니다.

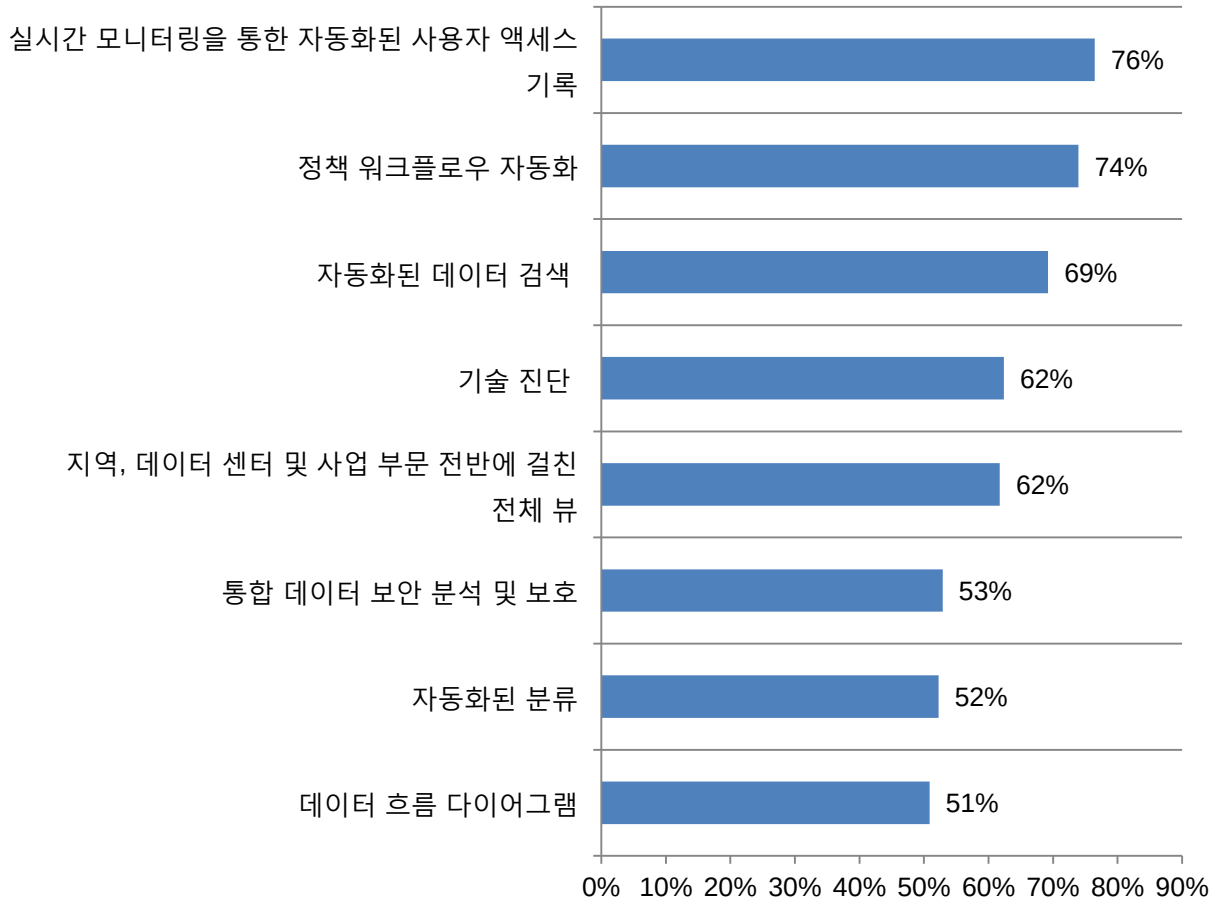
54%는 자동화된 프로세스 또는 제어를 통해 규정 위반을 방지할 수 있다고 생각하는 것으로 나타났습니다. 예산은 사고 위험을 줄이는 데 그다지 중요한 요소로 간주되지 않았습니다. 조직의 예산 또는 지출 규모를 확대하면 규정 위반 사고를 피할 수 있다고 응답한 응답자의 비율은 더 작았습니다(46%).

그림 12. 데이터 규정 위반 사고를 방지할 수 있는 방법
(매우 가능성이 높다 + 가능성이 있다)



전문 자동화된 솔루션이 조직의 규정 준수 및 데이터 보호 전략을 개선하는 데 도움이 된다고 생각하는 것으로 나타났습니다. 그림 13에는 대다수의 응답자가 보다 효과적인 규정 준수 및 데이터 보호 전략에 도움이 된다고 생각하는 8가지 데이터 중심 보안 기능이 나와 있습니다. 응답자들이 생각하는 가장 유용한 기능은 실시간 모니터링을 통한 자동화된 사용자 액세스 기록이었으며, 그 다음이 정책 워크플로우 자동화였습니다(각각 76%와 74%). 세 번째로는 69%의 응답자가 자동화된 데이터 검색이 유용하다고 응답했습니다.

그림 13. 다음 8가지 데이터 중심 보안 기능 중 규정 준수 및 데이터 보호를 개선하는 기능은 무엇입니까?
(매우 도움이 된다 + 도움이 된다)

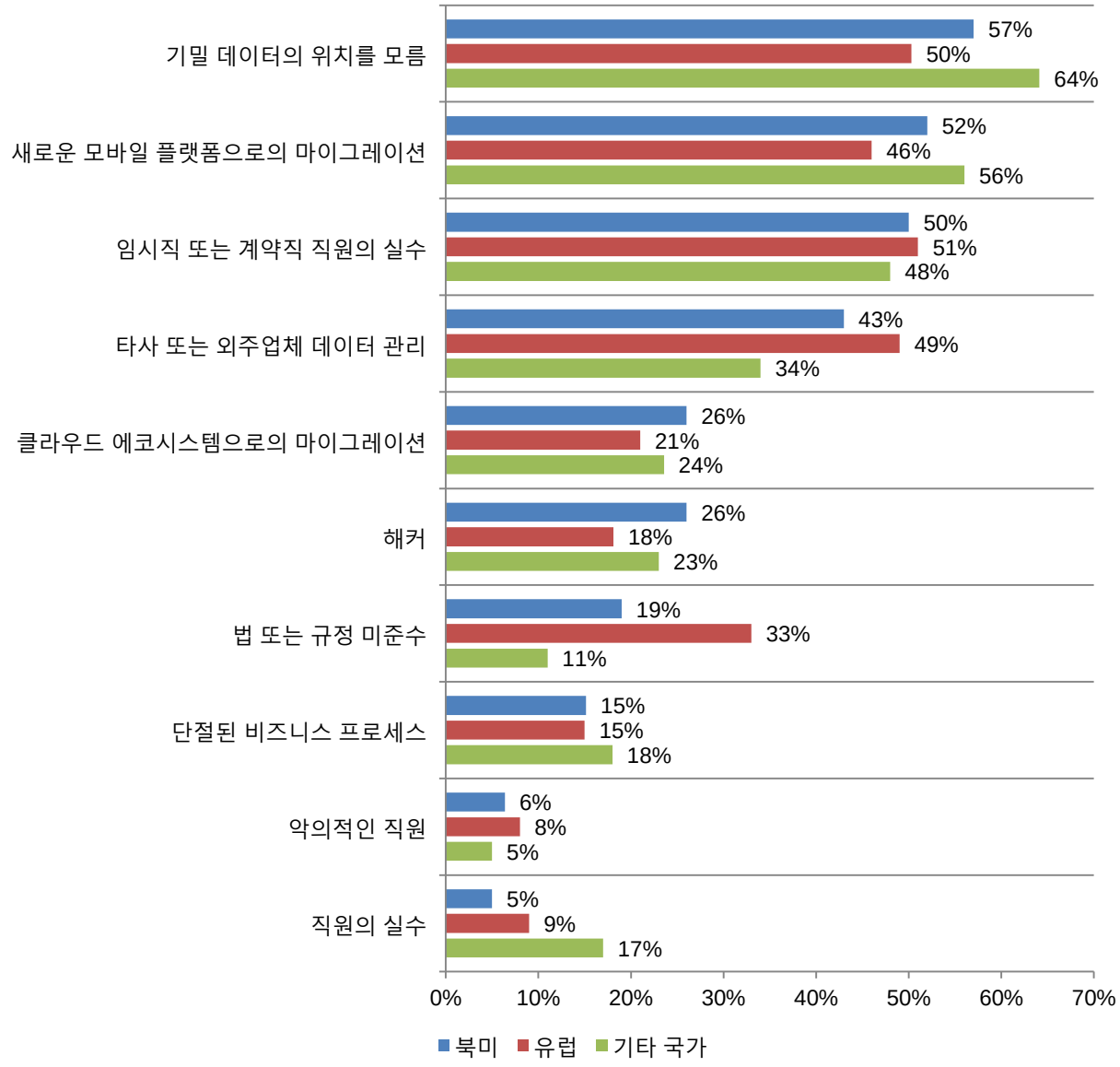


3부. 전세계 지역 간의 차이점

이 섹션에서는 본 조사에 참여한 국가 간의 가장 흥미로운 차이점에 대한 분석 결과를 제공합니다.

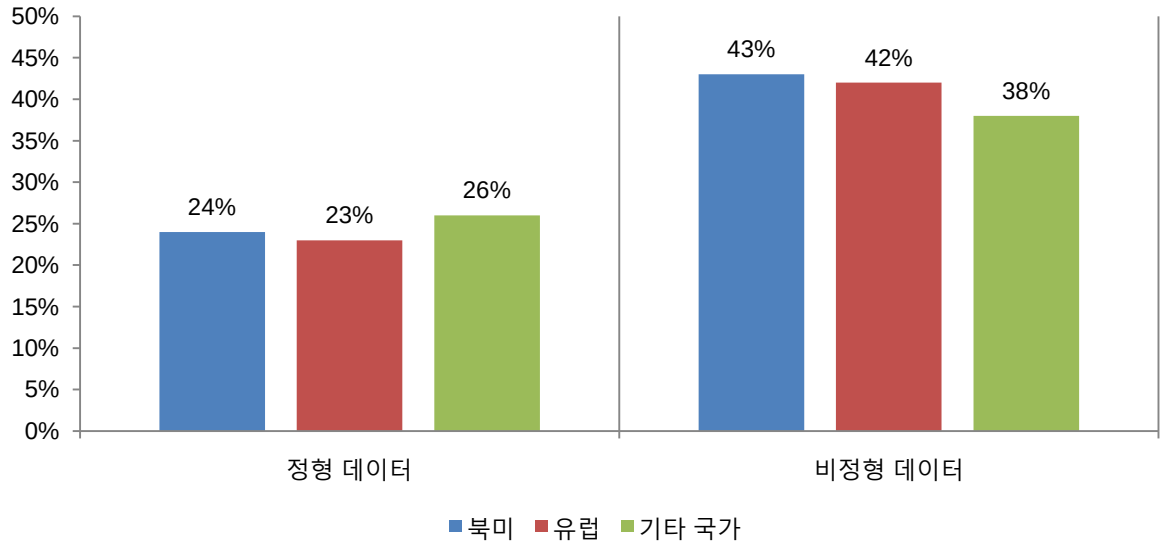
데이터 보안 상태에 대한 걱정 때문에 전세계의 응답자들이 야간 근무를 해야 한다고 응답했습니다. 그림 14에서는 대다수의 응답자들이 민감하거나 기밀인 데이터가 상주하는 곳을 모르기 때문에 조직의 데이터 자산에 대한 위협을 걱정하고 있음을 보여 줍니다. 기타 국가의 응답자들이 야간 근무에 가장 시달리는 반면, 유럽의 응답자들은 법 또는 규정 미준수를 더 우려하고 있는 것으로 나타났습니다.

그림 14. 야간 근무를 해야 하는 이유는 무엇입니까?
(최대 3개 선택)



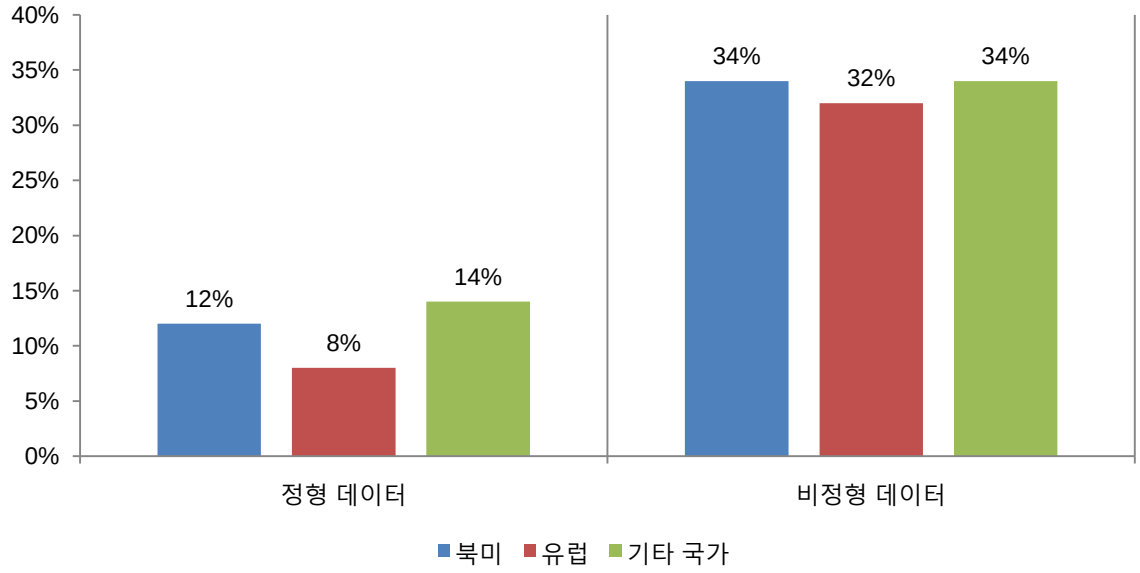
대부분의 조직이 민감하거나 기밀인 데이터가 있는 곳을 모르고 있습니다. 그림 15를 보면, 전체 응답자의 약 1/4만 민감한 정형 데이터가 있는 곳을 모두 알고 있다고 생각하는 것으로 나타났습니다. 특히 북미 응답자의 24%, 유럽 응답자의 23% 및 기타 국가 응답자의 26%는 데이터의 위치를 모르고 있습니다. 하지만 조직의 비정형 데이터가 있는 곳을 모르는 응답자의 비율은 그보다 훨씬 높게 나타났습니다.

그림 15. 데이터가 있는 곳을 아십니까?
('아니오'라고 응답한 비율)



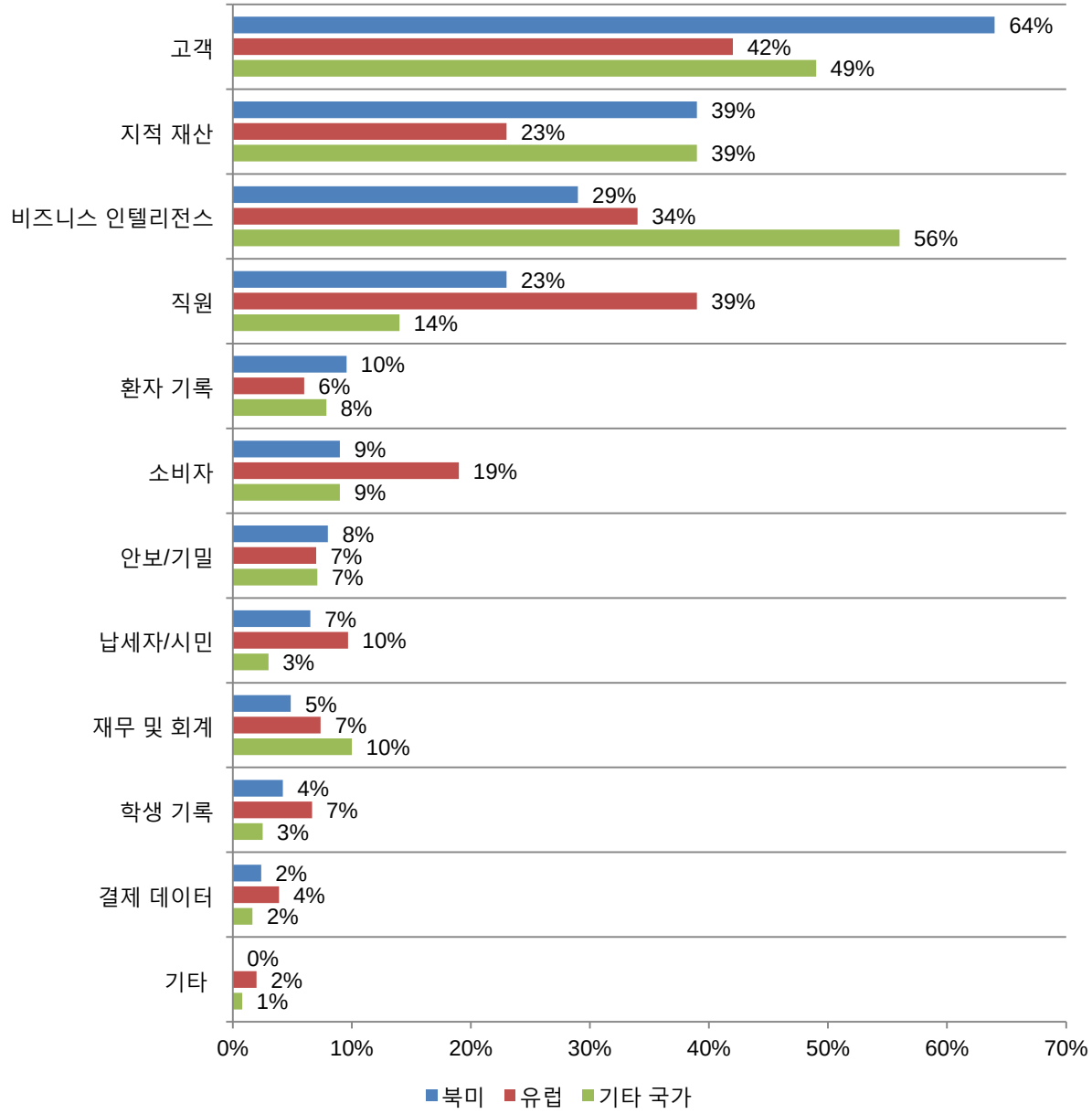
전세계적으로 비정형 데이터와 관련된 데이터 규정 위반을 감지하는 것이 어려운 것으로 나타났습니다. 그림 16에서는 데이터 규정 위반으로 인해 비정형 데이터가 손실되거나 도난된 경우보다 정형 데이터와 관련된 데이터 규정 위반을 감지하는 데 보다 자신이 있는 것을 보여 줍니다.

그림 16. 데이터 규정 위반을 감지할 수 있습니까?
('아니오'라고 응답한 비율)



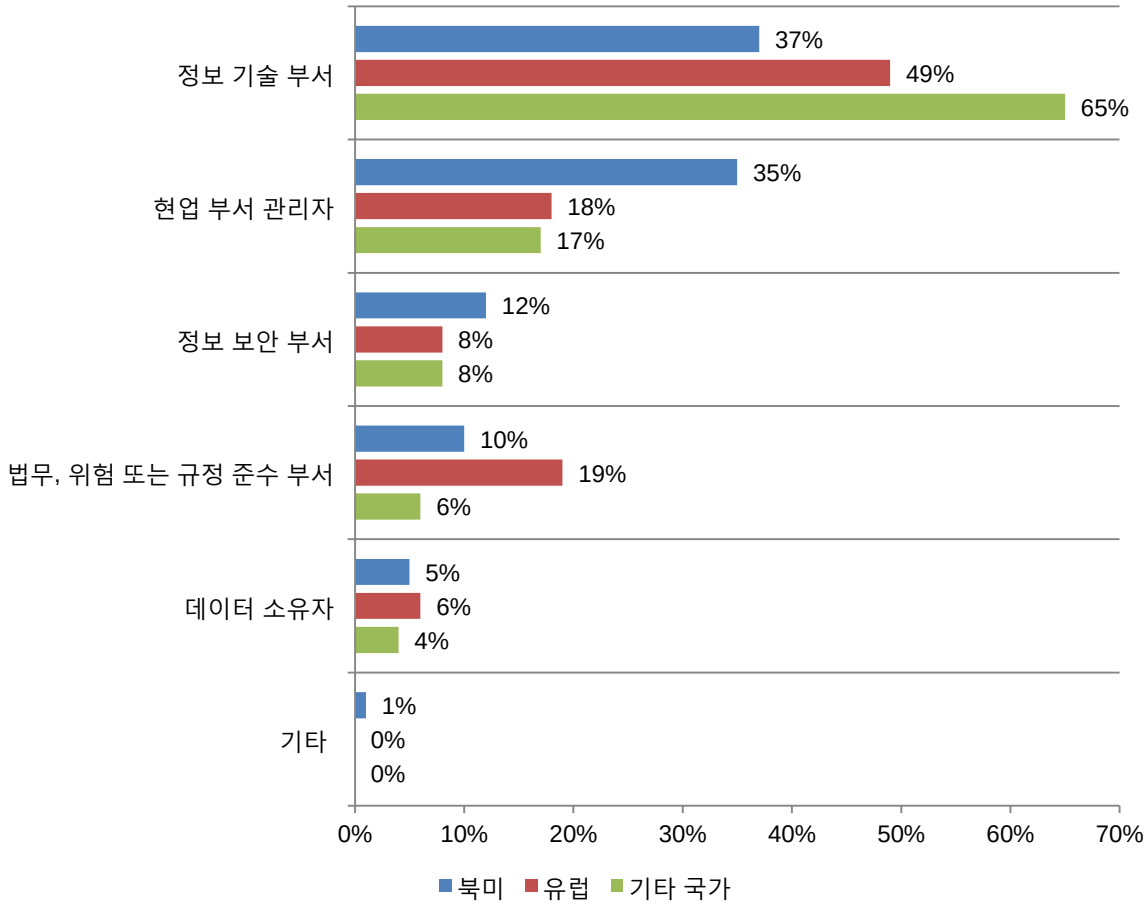
북미에서는 고객 데이터가 가장 위험한 것으로 간주되었습니다. 그림 17을 보면, 기타 국가에서도 고객 데이터가 취약하다고 응답한 것을 알 수 있습니다. 유럽의 응답자는 23%만 지적 재산을 우려하고 있었습니다. 흥미로운 것은, 기타 국가의 56% 응답자가 비즈니스 인텔리전스를 가장 위험한 것으로 간주했다는 점입니다.

그림 17. 조직에서 가장 위험한 것으로 간주되는 데이터
(최대 2개 선택)



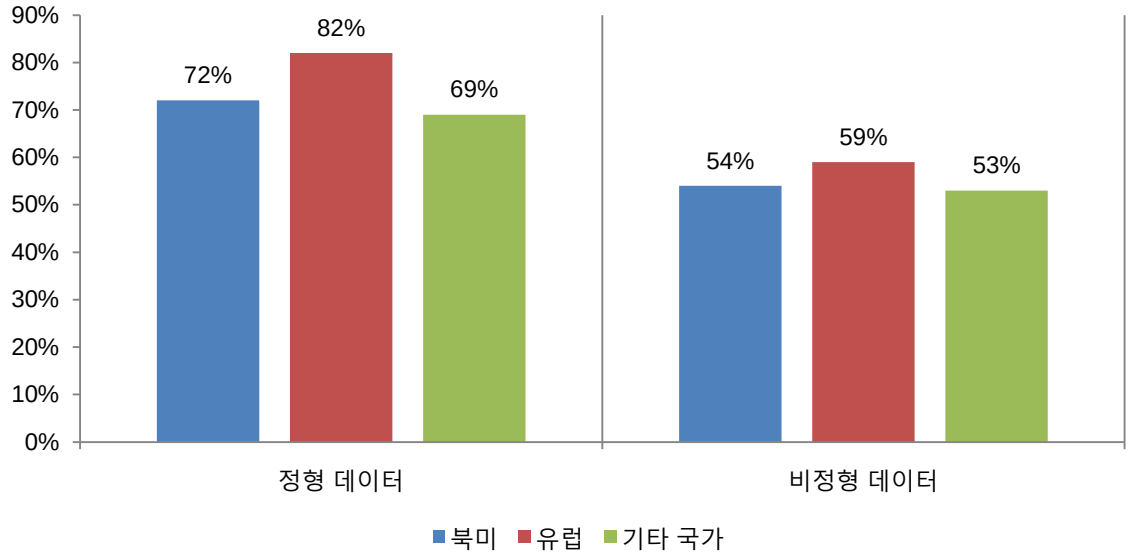
북미 이외 지역의 조직에서는 정보 기술 부서가 사용자에게 데이터 자산에 대한 액세스 권한을 부여하는 책임을 맡고 있었습니다. 반면, 북미 지역의 조직은 IT 부서와 현업 부서 관리자 간에 책임을 공유하는 경향이 있는 것으로 나타났습니다. 그림 18을 보면, 현업 부서 관리자의 영향력이 더 적은 것을 알 수 있습니다. 유럽의 경우 규정 미준수에 대한 우려 때문에 법무, 위험 또는 규정 준수 부서에서 책임을 맡고 있다고 응답한 응답자가 더 많았습니다.

그림 18. 사용자에게 데이터 자산에 대한 액세스 권한을 부여하는 책임은 누구에게 있습니까?
(최대 2개 선택)



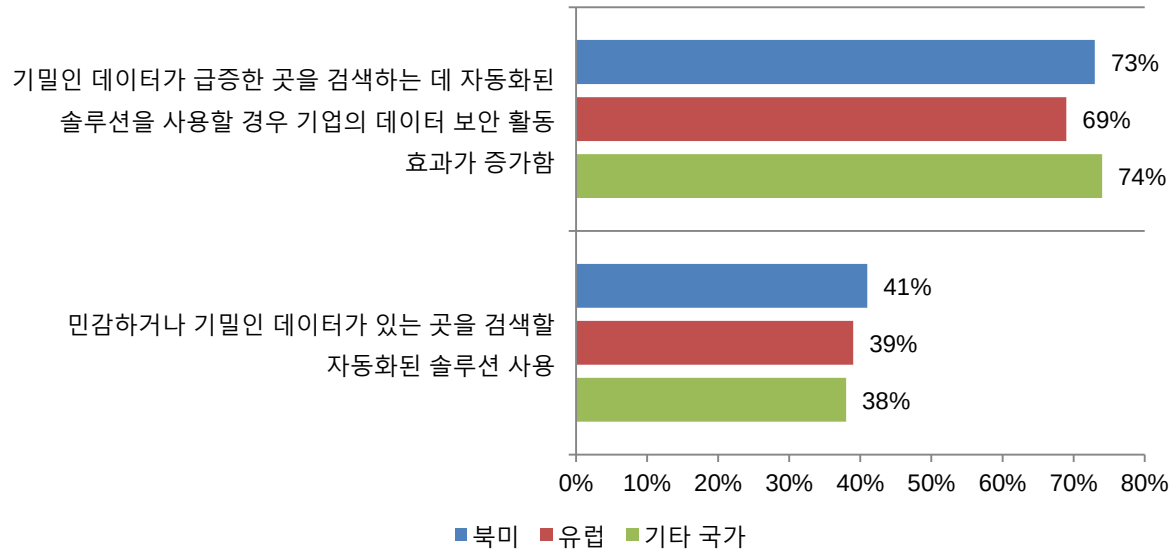
민감하거나 기밀인 정보에 대한 사용자 액세스를 파악하고 있다는 확신은 국가 간에 달랐습니다. 그림 19를 보면, 정형 데이터에 대한 사용자 액세스를 파악하는 능력에 있어 유럽의 조직이 가장 확신을 가지고 있고, 기타 국가의 조직이 가장 확신하지 못하는 것을 알 수 있습니다. 비정형 데이터에 대한 사용자 액세스 가시성은 모든 국가에서 확신하지 못하는 것으로 나타났습니다.

그림 19. 귀사에서 기밀 데이터에 대한 사용자 액세스를 파악하고 있다고 어느 정도 확신하십니까?
(매우 확신 + 확신)



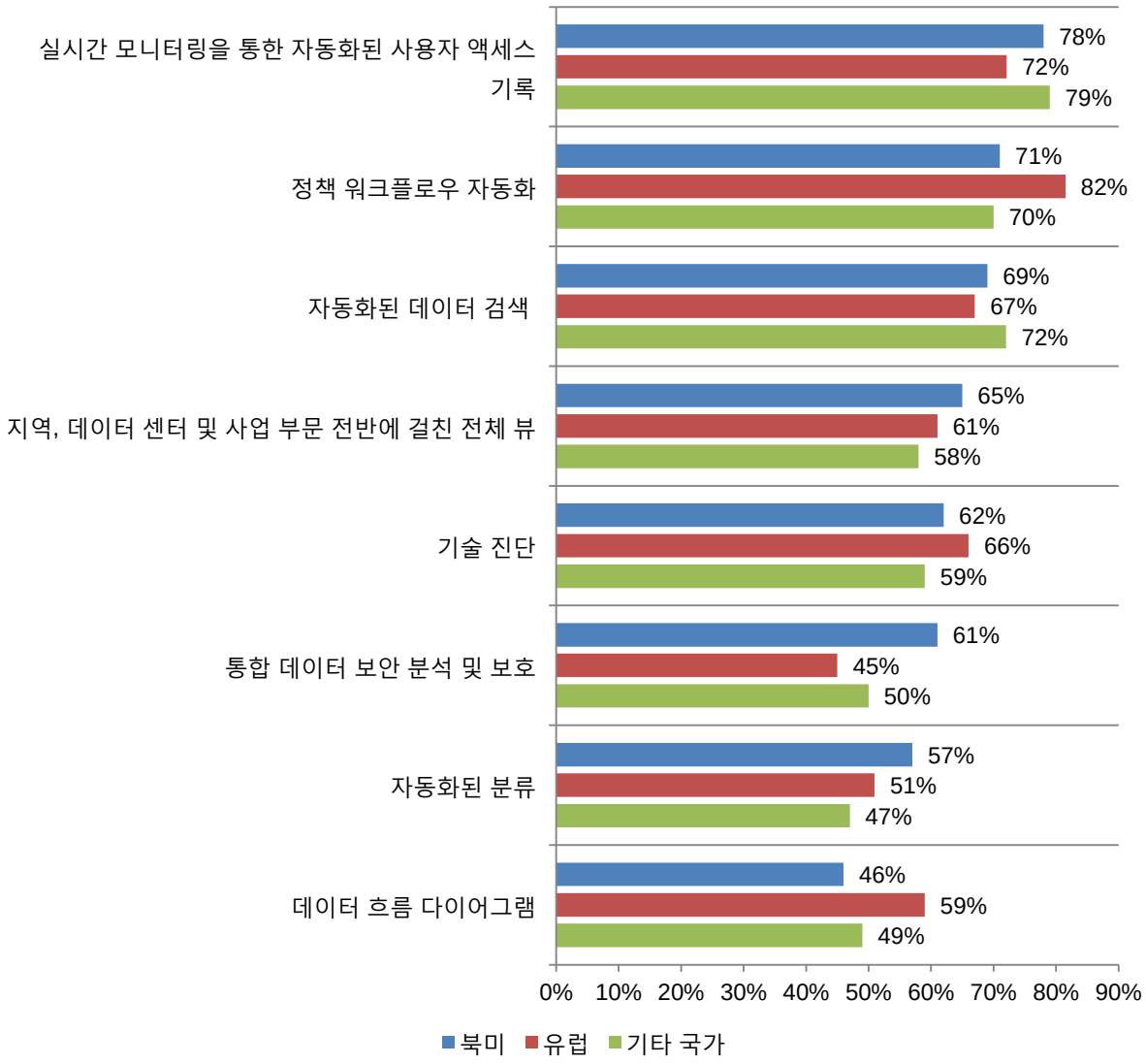
본 조사에 참여한 국가들은 민감하거나 기밀인 데이터가 급증하는 곳을 검색하기 위해 자동화된 솔루션을 사용하는 것에 긍정적인 것으로 나타났습니다. 이러한 솔루션을 사용하고 있는 비율은 낮았지만(북미의 경우 41%, 유럽의 경우 39%, 기타 국가의 경우 38%) 대다수의 응답자가 조직에서 민감하거나 기밀인 데이터가 급증하는 곳을 이해하는 데 매우 유용하다고 생각했습니다. 그림 20에서는 국가 간의 차이점을 보여 줍니다.

그림 20. 자동화된 솔루션의 사용
('예'라고 응답한 비율)



본 조사에 참여한 국가들은 가장 효과적인 데이터 중심 보안 기능에 대한 인식이 비슷한 것으로 나타났습니다. 그림 21에는 가장 중요한 세 가지 기능이 실시간 모니터링을 통한 자동화된 사용자 액세스 기록, 정책 워크플로우 자동화 및 자동화된 데이터 검색인 것으로 나타나 있습니다.

그림 21. 다음 8가지 데이터 중심 보안 기능 중 규정 준수 및 데이터 보호를 개선하는 기능은 무엇입니까?
(매우 도움이 된다 + 도움이 된다)



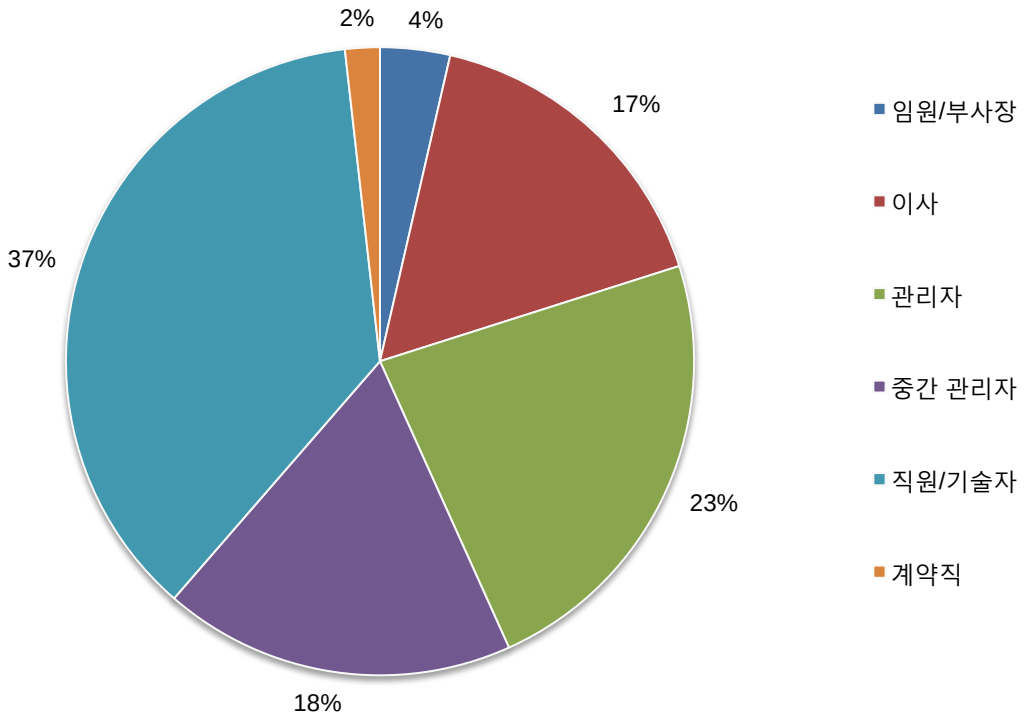
4부. 방법 및 제한

표 1에는 북미, 유럽 및 기타 국가에 대한 종합적인 표본 응답이 나와 있습니다. 16개국의 총 45,829명에 이르는 IT 및 IT 보안 실무자에게 본 글로벌 조사에 참여해 달라고 요청한 결과, 총 1,743명의 응답자가 설문 조사를 제출해 주었습니다. 그 중 신뢰도와 선별성 검사에서 156명의 응답이 제외되었습니다. 따라서 최종 표본은 1,587명이었으며, 이는 3.5%의 응답률에 해당합니다.

표 1. 표본 응답	표본 수	비율(%)
총 표본	45,829	100%
총 응답자	1,743	3.8%
거부 및 검열된 응답자	156	0.3%
최종 표본	1,587	3.5%

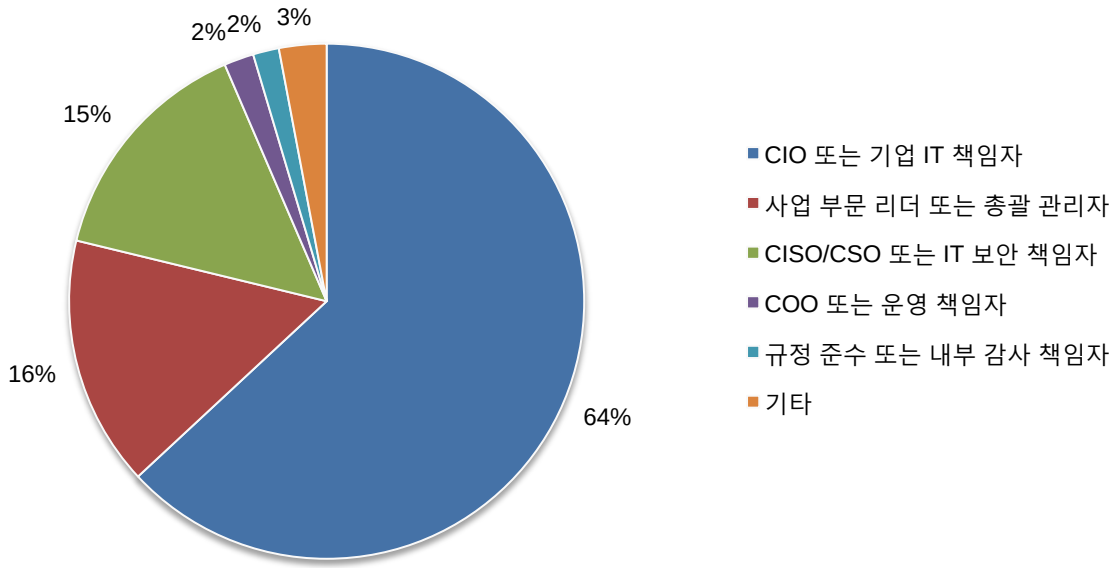
원형 차트 1에서 응답자들의 조직 내 직위를 보여 줍니다. 의도한 대로 응답자의 61%가 중간 관리자 이상의 직위를 가지고 있습니다.

원형 차트 1. 조직 내 현재 직위
통합 뷰



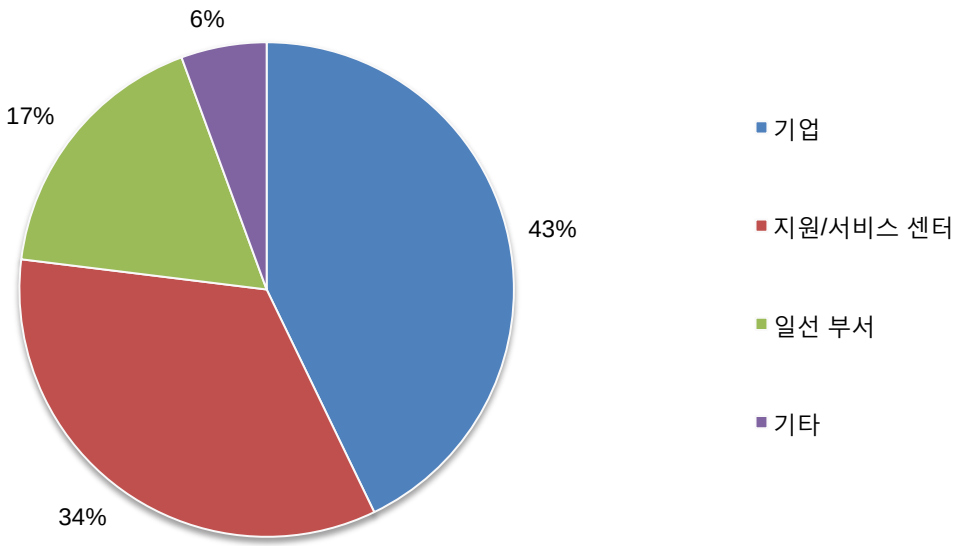
원형 차트 2에서는 응답자들의 조직 내 직속 상관을 보여 줍니다. 응답자의 64%가 CIO 또는 기업 IT 책임자라고 응답했습니다.

원형 차트 2. 직속 상관
통합 뷰



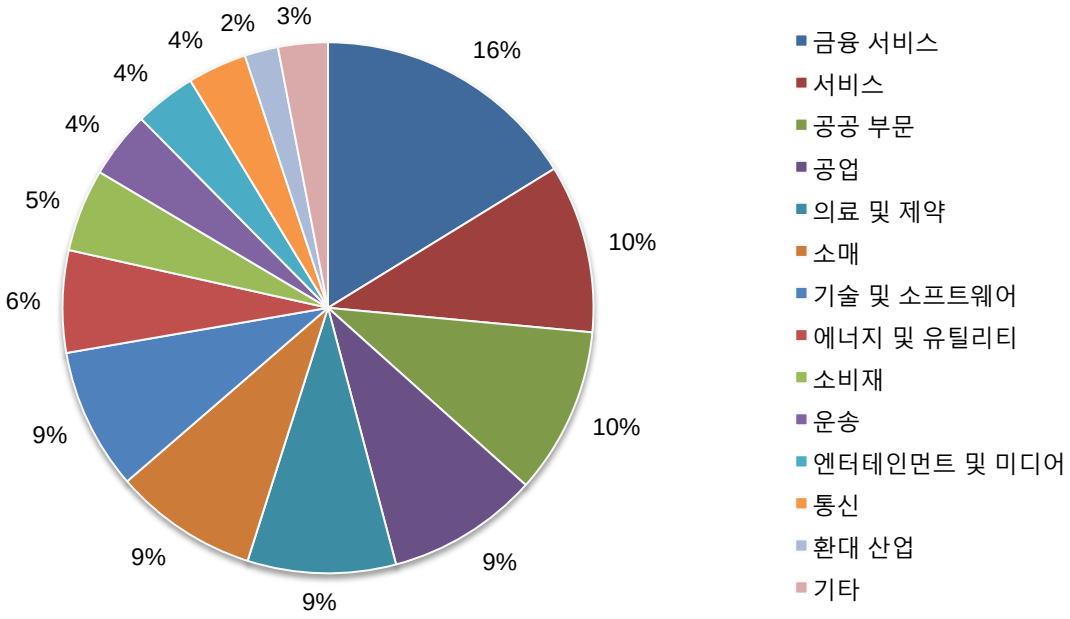
원형 차트 3을 보면, 응답자의 43%가 자신의 직무 또는 역할 범위를 기업이라고 응답한 것을 알 수 있습니다. 34%는 지원/서비스 센터라고 응답했습니다.

원형 차트 3. 직무 또는 역할 범위
통합 뷰



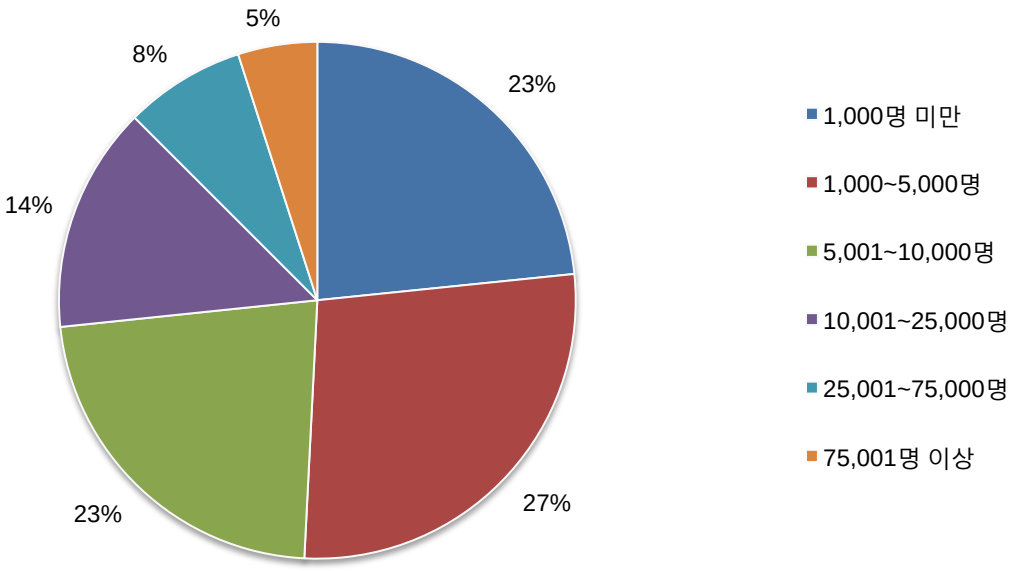
원형 차트 4에서는 응답자 조직의 산업 분류를 보여 줍니다. 이 차트에는 금융 서비스(16%)가 가장 큰 부분을 차지하고 있고, 그 다음이 서비스(10%)와 공공 부문(10%)입니다.

원형 차트 4. 주 산업 분류
통합 뷰



원형 차트 5를 보면, 응답자의 50%가 해당 조직의 전세계 직원 수가 5,000명 이상인 것을 알 수 있습니다.

원형 차트 5. 글로벌 조직의 정규직 직원 수
통합 뷰



5부. 본 조사의 유의 사항

본 설문 조사에는 결과에서 추론을 도출하기 전에 신중하게 고려해야 하는 내재된 제한이 있습니다. 다음 항목은 대부분의 웹 기반 설문 조사와 밀접한 관련이 있는 특정 제한입니다.

- 무응답 바이어스: 현재 결과는 반환된 설문 조사 표본을 기반으로 합니다. 본 조사에서는 유용한 수의 응답을 얻기 위해 대표적인 개인 표본에게 보냈으며, 참여하지 않은 사람들의 생각은 설문을 작성한 응답자들의 기본적인 생각과 상당히 다를 수 있습니다.

- 표본 추출 바이어스: 정확성은 IT 또는 IT 보안 실무자를 대표하는 정도 및 연락처 정보를 기반으로 합니다. 또한 언론 보도와 같은 외부 이벤트에 의해 결과가 편향될 수도 있음을 인정합니다. 끝으로 본 조사에서는 웹 기반 수집 방법을 사용했기 때문에 우편이나 전화 통화로 실시하는 설문 조사와 결과의 패턴이 다를 수 있습니다.

- 자체 보고된 결과: 본 설문 조사의 품질은 응답자로부터 받은 기밀 응답의 무결성을 기반으로 합니다. 확인 및 조정을 설문 조사 과정에 포함할 수 있지만 응답자가 항상 정확한 응답만을 제공하는 것은 아닙니다.

부록: 자세한 설문 조사 결과

다음 표에서는 본 조사에 포함된 모든 문항에 대한 종합적인 응답자 수 또는 응답 비율을 제공합니다. 모든 설문 조사 응답은 2014년 4월에 취합되었습니다.

설문 조사 응답	결과
총 표본	45,829
총 응답자	1,743
거부되거나 검열된 응답자	156
최종 표본	1,587
응답률	3.5%

1부: 선별 질문

S1. 귀하의 직무는 민감하거나 기밀인 비즈니스 정보 보호와 관련이 있습니까?	결과
예	100%
아니오(중지)	0%
합계	100%

S2. 다음 중 귀하의 직무에 대한 가장 올바른 정의는 무엇입니까?	결과
조직 내 데이터를 보호해야 하는 책임자	18%
조직 내 데이터 보호 활동에 전념	24%
조직 내 데이터 보호 활동에 일부 참여	32%
조직 내 데이터 보호 활동에 관여	26%
참여하거나 관여하지 않음(중지)	0%
합계	100%

S3a. 귀하의 직무는 **정형** 데이터(예: 데이터베이스에 포함된 데이터)의 보호와 어느 정도 관련이 있습니까?	결과
0(중지)	0%
5% 미만	6%
5~10%	23%
11~25%	33%
26~50%	19%
51~75%	14%
76~100%	4%
합계	100%

S3b. 귀하의 직무는 **비정형** 데이터(예: 전자 메일 및 파일 내 데이터)의 보호와 어느 정도 관련이 있습니까?	결과
0(중지)	0%
5% 미만	9%
5~10%	36%
11~25%	31%
26~50%	12%
51~75%	6%
76~100%	6%
합계	100%

2부: 문제점

Q1. 귀사의 보안 상태를 고려할 때 **귀하가 야간 근무를 해야 하는 이유는 무엇입니까**? 가장 올바른 항목 3개를 선택하십시오.	결과
민감하거나 기밀인 데이터의 위치를 모름	57%
해커	23%
악의적인 직원	6%
단절된 비즈니스 프로세스	16%
직원의 실수	10%
임시직 또는 계약직 직원의 실수	50%
타사 또는 외주업체 데이터 관리(클라우드 포함)	42%
법 또는 규정 미준수	21%
클라우드 에코시스템으로의 마이그레이션	24%
새로운 모바일 플랫폼으로의 마이그레이션	51%
합계	300%

Q2a. 귀사의 민감하거나 기밀인 **정형 데이터**(예: 데이터베이스에 있는 데이터)가 어디에 있는지 아십니까? (운영계, 테스트, 지원 또는 데이터 웨어하우스 포함)	결과
예, 모든 데이터	16%
예, 대부분의 데이터	22%
예, 일부 데이터	38%
아니오	24%
합계	100%

Q2b. '아니오'라고 응답한 경우, 위치를 **알 수 없는** 조직의 민감하거나 기밀인 **정형 데이터**는 몇 퍼센트입니까? 최대한 추측해 주십시오.	결과
0	0%
5% 미만	6%
5~10%	24%
11~25%	28%
26~50%	29%
51~75%	10%
76~100%	3%
합계	100%

Q3a. 귀사의 민감하거나 기밀인 **비정형 데이터**(예: 전자 메일 또는 파일에 있는 데이터)가 어디에 있는지 아십니까?	결과
예, 모든 데이터	7%
예, 대부분의 데이터	10%
예, 일부 데이터	42%
아니오	41%
합계	100%

Q3b. '아니오'라고 응답한 경우, 위치를 **알 수 없는** 조직의 민감하거나 기밀인 **비정형 데이터**는 몇 퍼센트입니까? 최대한 추측해 주십시오.	결과
0	0%
5% 미만	3%
5~10%	8%
11~25%	16%
26~50%	25%
51~75%	27%
76~100%	21%
합계	100%

Q4a. 귀사에서 **정형 데이터**와 관련된 데이터 규정 위반이 발생한 경우 이를 감지할 수 있습니까?	결과
예, 항상 감지할 수 있음	26%
예, 대부분 감지할 수 있음	34%
예, 일부 감지할 수 있음	29%
아니오	11%
합계	100%

0%

Q4b. 귀사에서 **비정형 데이터**와 관련된 데이터 규정 위반이 발생한 경우 이를 감지할 수 있습니까?	결과
예, 항상 감지할 수 있음	12%
예, 대부분 감지할 수 있음	22%
예, 일부 감지할 수 있음	33%
아니오	33%
합계	100%

개인적인 의견: 아래에 제공된 척도를 사용하여 민감하거나 기밀인 데이터에 대한 각 설명에 어느 정도 공감하는지 평가하십시오. (매우 그렇다 + 그렇다)	결과
Q5a. 내 조직의 민감하거나 기밀인 정보가 있는 곳을 모른다는 것은 보안 위험이 크다는 것을 나타냄	79%
Q5b. 내 조직에서 데이터 보안 및/또는 보호는 우선 순위가 높은 해결 과제임	51%
Q5c. 내 조직에는 정규직, 임시직 또는 계약직 직원이 데이터에 **지나치게 자주** 액세스할 위험이 거의 없음	23%
Q5d. 내 조직에는 민감한 데이터에 대한 액세스가 역할, 위치 및/또는 기타 요소별로 제어됨	42%

Q6. 데이터가 손실되거나 도난될 경우 귀사에 가장 큰 위험이 될 수 있는 데이터의 유형은 무엇입니까? 가장 중요한 항목 2개를 선택하십시오.	결과
고객	53%
지적 재산	34%
비즈니스 인텔리전스	38%
직원	25%
환자 기록	8%
소비자	12%
안보/기밀	7%
납세자/시민	6%
재무 및 회계	7%
학생 기록	4%
결제 데이터(예: 신용 카드 번호)	3%
기타(구체적으로 기재)	1%
합계	200%

Q7. 민감하거나 기밀인 것으로 간주되는 조직의 데이터는 몇 퍼센트입니까(정형 및 비정형을 비롯한 모든 소스 고려)?	결과
5% 미만	3%
5~10%	21%
11~25%	36%
26~50%	13%
51~75%	10%
76~100%	17%
합계	100%

Q8. 사용자에게 데이터 자산에 대한 액세스 권한을 부여하는 책임은 누구에게 있습니까? 2개만 선택하십시오.	결과
정보 기술 부서	49%
정보 보안 부서	10%
법무, 위험 또는 규정 준수 부서	12%
현업 부서 관리자	25%
데이터 소유자	5%
기타(구체적으로 기재)	0%
합계	100%

Q9a. 민감하거나 기밀인 **정형 데이터** 자산의 안전한 사용을 고려할 때 귀사에 필요한 기술 또는 "툴"은 무엇입니까?	결과
데이터베이스 활동 모니터링(DAM)	47%
민감한 데이터 분류	68%
데이터베이스 암호화	47%
민감한 필드의 투명한 토큰화	20%
개발계 환경의 민감한 필드에 대한 영구 마스킹	25%
운영계 환경의 민감한 필드에 대한 동적 마스킹	13%
애플리케이션 수준 액세스 제어	62%
데이터베이스 및 엔터프라이즈 애플리케이션의 데이터에 대한 중앙 집중식 액세스 제어	42%

Q9b. 민감하거나 기밀인 **비정형 데이터** 자산의 안전한 사용을 고려할 때 귀사에 필요한 기술 또는 "툴"은 무엇입니까? 해당하는 항목을 모두 선택하십시오.	결과
데이터 손실 방지(DLP)	29%
민감한 데이터 분류	54%
ID 및 액세스 관리	31%
디지털 권한 관리	29%
중앙 집중식 액세스 제어 관리 및 권한 부여	19%
파일 시스템 및 액세스 감사	14%
보안 정보 관리(SIM)	40%

Q10a. 귀사에서 민감하거나 기밀인 **정형 데이터**에 대한 사용자 액세스를 파악하고 있다고 얼마나 확신하십니까?	결과
매우 확신	34%
확신	40%
확신 못함	26%
합계	100%

Q10b. 귀사에서 민감하거나 기밀인 **비정형 데이터**에 대한 사용자 액세스를 파악하고 있다고 얼마나 확신하십니까?	결과
매우 확신	21%
확신	34%
확신 못함	45%
합계	100%

Q11. 귀사에서는 아래 나열된 절차에 따라 데이터 자산의 허용되는 사용을 얼마나 잘 관리하고 있습니까? 매우 잘 이행부터 수립되어 있지 않음까지 5점 척도로 평가하십시오.	
데이터 보안 절차 [데이터베이스]	결과
민감하고 기밀인 데이터가 있는 위치 파악 및 추적	45%
데이터 아키텍처 구성(맵, 계보, 흐름 및 인벤토리 포함)	50%
우선 순위 지정을 통해 데이터 분류 관리	40%
직무, 역할 또는 알아야 할 필요성에 따른 액세스 권한 모니터링	48%
정책 변경, 사용자 요구 사항 또는 애플리케이션 업데이트에 따른 액세스 변경 관리	53%
직원의 퇴사 또는 정책 변경 시 데이터 액세스 권한 철회	51%
애플리케이션, 위치, 부서, 기술 표준 전반에 걸쳐 일관된 방식으로 데이터 액세스 정책 적용	59%
정형 및 비정형 데이터에서 권한 있는 사용자의 데이터 액세스 모니터링	49%
임무 분리 모니터링	27%
정책 및 규정 준수 증거 제공	35%
허용되는 사용 정책 생성	30%
클라우드를 포함하여 타사와 주고 받는 데이터 전송 모니터링	61%
데이터 액세스 및 제어 정책에 대해 최종 사용자 교육	47%
데이터 유출 또는 도난 감지 및 포함(데이터 규정 위반)	45%
데이터 손실 방지 솔루션 구현	45%
암호화 및/또는 토큰화로 민감한 데이터 보호	42%
마스킹, 데이터 식별 불가, 데이터 수정 또는 데이터 비표시로 민감한 데이터 보호	56%
포괄적인 디지털 포렌식 기능	65%

데이터 보안 절차 [전자 메일]	결과
민감하고 기밀인 데이터가 있는 위치 파악 및 추적	56%
데이터 아키텍처 구성(맵, 계보, 흐름 및 인벤토리 포함)	56%
우선 순위 지정을 통해 데이터 분류 관리	44%
직무, 역할 또는 알아야 할 필요성에 따른 액세스 권한 모니터링	59%
정책 변경, 사용자 요구 사항 또는 애플리케이션 업데이트에 따른 액세스 변경 관리	57%
직원의 퇴사 또는 정책 변경 시 데이터 액세스 권한 철회	59%
애플리케이션, 위치, 부서, 기술 표준 전반에 걸쳐 일관된 방식으로 데이터 액세스 정책 적용	62%
정형 및 비정형 데이터에서 권한 있는 사용자의 데이터 액세스 모니터링	60%
임무 분리 모니터링	40%
정책 및 규정 준수 증거 제공	44%
허용되는 사용 정책 생성	33%
클라우드를 포함하여 타사와 주고 받는 데이터 전송 모니터링	38%
데이터 액세스 및 제어 정책에 대해 최종 사용자 교육	55%
데이터 유출 또는 도난 감지 및 포함(데이터 규정 위반)	63%
데이터 손실 방지 솔루션 구현	45%
암호화 및/또는 토큰화로 민감한 데이터 보호	49%
마스킹, 데이터 식별 불가, 데이터 수정 또는 데이터 비표시로 민감한 데이터 보호	68%
포괄적인 디지털 포렌식 기능	69%

데이터 보안 절차 [파일]	결과
민감하고 기밀인 데이터가 있는 위치 파악 및 추적	51%
데이터 아키텍처 구성(맵, 계보, 흐름 및 인벤토리 포함)	58%
우선 순위 지정을 통해 데이터 분류 관리	49%
직무, 역할 또는 알아야 할 필요성에 따른 액세스 권한 모니터링	63%
정책 변경, 사용자 요구 사항 또는 애플리케이션 업데이트에 따른 액세스 변경 관리	63%
직원의 퇴사 또는 정책 변경 시 데이터 액세스 권한 철회	64%
애플리케이션, 위치, 부서, 기술 표준 전반에 걸쳐 일관된 방식으로 데이터 액세스 정책 적용	67%
정형 및 비정형 데이터에서 권한 있는 사용자의 데이터 액세스 모니터링	63%
임무 분리 모니터링	42%
정책 및 규정 준수 증거 제공	43%
허용되는 사용 정책 생성	40%
클라우드를 포함하여 타사와 주고 받는 데이터 전송 모니터링	72%
데이터 액세스 및 제어 정책에 대해 최종 사용자 교육	58%
데이터 유출 또는 도난 감지 및 포함(데이터 규정 위반)	56%
데이터 손실 방지 솔루션 구현	62%
암호화 및/또는 토큰화로 민감한 데이터 보호	48%
마스킹, 데이터 식별 불가, 데이터 수정 또는 데이터 비표시로 민감한 데이터 보호	64%
포괄적인 디지털 포렌식 기능	68%

Q12a. 조직에서 현재 자동화된 솔루션을 사용하여 민감하거나 기밀인 데이터가 있는 곳을 검색합니까?	결과
예	40%
아니오	60%
합계	100%

Q12b. '예'라고 응답한 경우, 데이터베이스 및 엔터프라이즈 애플리케이션에서 민감하거나 기밀인 데이터가 있는 곳을 검색할 자동화된 솔루션이 있습니까?	결과
예	64%
아니오	36%
합계	100%

Q12c. '예'라고 응답한 경우, 파일 및 전자 메일에서 민감하거나 기밀인 데이터가 있는 곳을 검색할 자동화된 솔루션이 있습니까?	결과
예	22%
아니오	78%
합계	100%

Q12d. '아니오'라고 응답한 경우, 민감하거나 기밀인 데이터 검색에 자동화된 솔루션을 사용하면 데이터 보안 활동의 효과가 증가할 것이라고 생각하십니까?	결과
예	78%
아니오	22%
합계	100%

Q12e. 민감하거나 기밀인 데이터가 급증한 곳을 검색하는 데 자동화된 솔루션을 사용할 경우 기업의 데이터 보안 활동 효과가 증가할 것이라고 생각하십니까?	결과
예	72%
아니오	28%
합계	100%

Q13a. 조직에서 지난 12개월 동안 데이터 규정 위반이 발생한 적이 있습니까?	결과
예, 1번 있음	27%
예, 2~5번 있음	18%
예, 6번 이상 있음	4%
아니오(Q14로 건너뜀)	51%
합계	100%

Q13b. (매우 가능성이 높다 + 가능성이 있다)	결과
Q13b-1. '예'라고 응답한 경우, 조직에 보다 효과적인 **데이터 보안 기술이** 있었다면 이러한 규정 위반 사고를 피할 수 있었을 것이라고 생각하십니까?	58%
Q13b-2. '예'라고 응답한 경우, 조직의 **예산** 또는 지출 규모가 더 컸더라면 이러한 규정 위반 사고를 피할 수 있었을 것이라고 생각하십니까?	46%
Q13b-3. '예'라고 응답한 경우, 조직에 보다 숙련된 데이터 보안 **책임자**가 있었더라면 이러한 규정 위반 사고를 피할 수 있었을 것이라고 생각하십니까?	57%
Q13b-4. '예'라고 응답한 경우, 조직에 보다 **자동화된 프로세스** 또는 제어 기능이 있었다면 이러한 규정 위반 사고를 피할 수 있었을 것이라고 생각하십니까?	54%

Q14. 다음 중 귀사의 규정 준수 및 데이터 보호 전략을 개선하는 데 도움이 된다고 생각하는 기능은 무엇입니까? 각 항목 아래에 제공된 척도를 사용하여 각 기능에 대한 답을 작성하십시오. (매우 도움이 된다 + 도움이 된다)	결과
Q14a. 자동화된 데이터 검색	69%
Q14b. 자동화된 분류	52%
Q14c. 실시간 모니터링을 통한 자동화된 사용자 액세스 기록	76%
Q14d. 지역, 데이터 센터 및 사업 부문 전반에 걸친 전체 뷰	62%
Q14e. 데이터 흐름 다이어그램	51%
Q14f. 기술 진단(취약점 평가 툴 포함)	62%
Q14g. 통합 데이터 보안 분석 및 보호	53%
Q14h. 정책 워크플로우 자동화	74%

3부. 표본 특성	
D1. 조직 내 귀하의 직함을 가장 잘 설명하는 것은 무엇입니까?	결과
임원/부사장	4%
이사	17%
관리자	23%
중간 관리자	18%
직원/기술자	37%
계약직	2%
기타(구체적으로 기재)	0%
합계	100%

D2. 귀하의 직속 상관을 가장 잘 설명하는 것은 무엇입니까?	결과
CEO/경영 위원	1%
COO 또는 운영 책임자	2%
CFO, 회계 감사관 또는 재무 책임자	1%
CIO 또는 기업 IT 책임자	64%
사업 부문 리더 또는 총괄 관리자	16%
규정 준수 또는 내부 감사 책임자	2%
CISO/CSO 또는 IT 보안 책임자	15%
CPO 또는 기업 보안 책임자	1%
기타(구체적으로 기재)	0%
합계	100%

D3. 귀하의 직무 또는 역할의 지리적 범위를 가장 잘 설명하는 것은 무엇입니까?	결과
전세계	48%
한 나라 이상	38%
특정 지역	14%
합계	100%

D4. 귀하의 직무 또는 역할 범위를 가장 잘 설명하는 것은 무엇입니까?	결과
기업	43%
일선 부서	17%
지원/서비스 센터	34%
기타(구체적으로 기재)	6%
합계	100%

D6. 귀사의 주 산업 분류를 가장 잘 설명하는 것은 무엇입니까?	결과
농업 및 음식 서비스	1%
통신	4%
소비재	5%
국방 및 우주항공	0%
교육 및 연구	1%
에너지 및 유틸리티	6%
엔터테인먼트 및 미디어	4%
금융 서비스	16%
의료 및 제약	9%
환대 산업	2%
공업	9%
공공 부문	10%
소매	9%
서비스	10%
기술 및 소프트웨어	9%
운송	4%
기타(구체적으로 기재)	1%
합계	100%

D5. 귀사의 전세계 정규직 직원 수는 다음 중 어느 범위에 속합니까?	결과
1,000명 미만	23%
1,000~5,000명	27%
5,001~10,000명	23%
10,001~25,000명	14%
25,001~75,000명	8%
75,001명 이상	5%
합계	100%

국가

D6. 현재 거주지는 어디입니까(국가 목록)?	결과
아르헨티나	67
호주	89
브라질	54
캐나다	142
프랑스	45
독일	165
홍콩	39
이탈리아	55
일본	82
멕시코	55
네덜란드	71
싱가포르	26
대한민국	41
스페인	46
영국	109
미국	501
합계	1,587

Ponemon Institute

책임 있는 정보 관리 개선

Ponemon Institute는 기업 및 정부 내의 책임 있는 정보 및 개인 정보 관리 관행을 개선하는 독립적인 연구 및 교육에 전념하고 있습니다. Ponemon Institute의 사명은 개인과 조직에 대한 민감한 정보의 관리 및 보안에 영향을 주는 중요한 문제에 대해 뛰어난 품질의 실증적 연구를 수행하는 것입니다.

CASRO(Council of American Survey Research Organizations)의 회원사인 Ponemon Institute는 엄격한 데이터 기밀, 개인 정보 및 윤리적 연구 기준을 준수합니다. Ponemon Institute는 개인으로부터 어떠한 개인 식별 정보(또는 기업 조사의 경우 기업 식별 정보)도 수집하지 않습니다. 아울러 조사 대상에게 본질에서 벗어나거나 관련이 없거나 부적절한 질문을 하지 않도록 엄격한 품질 기준을 준수합니다.