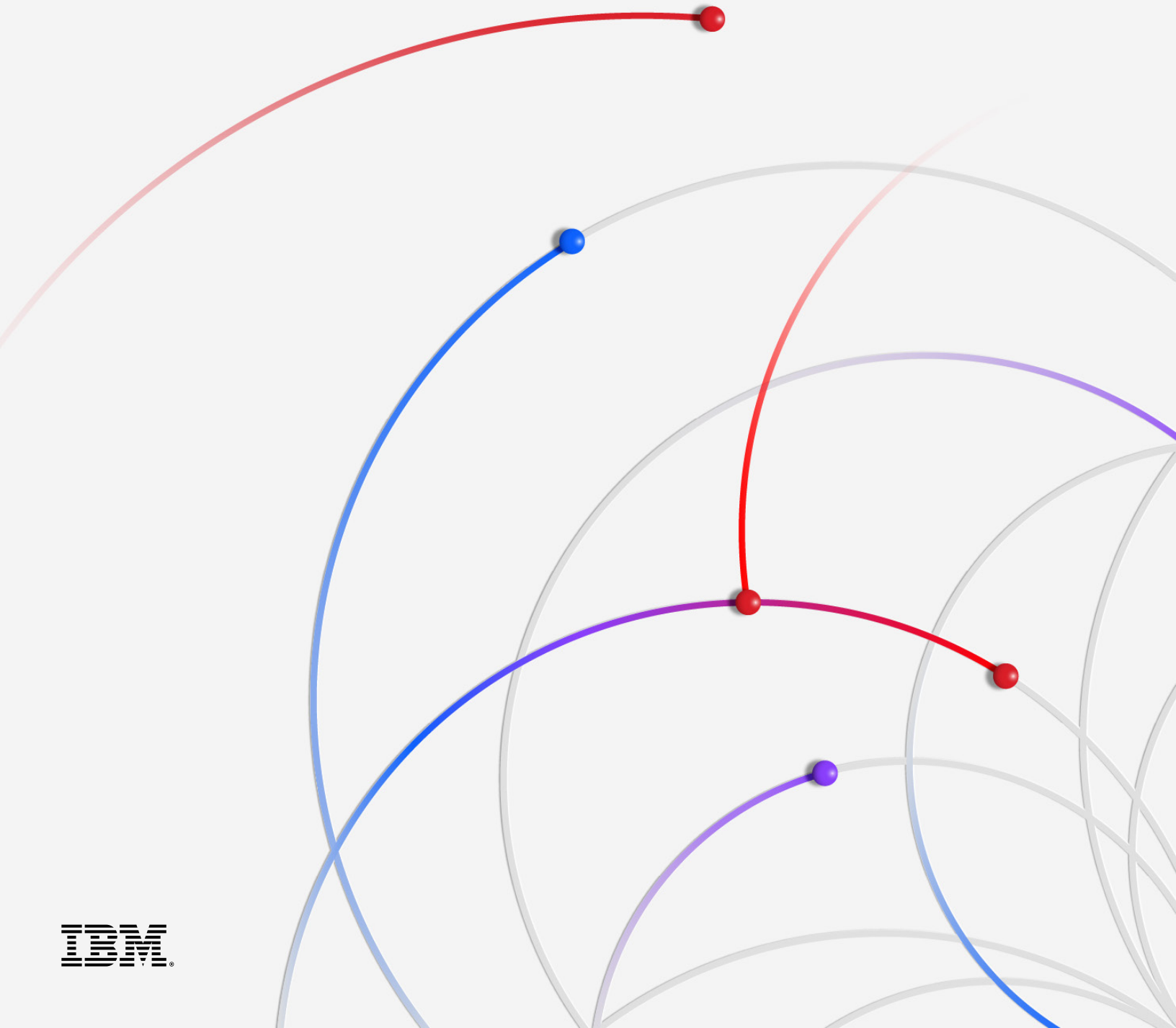
데이터 유출 비용 보고서 2024



IBM

목차

3 **개요**
4 2024년도 보고서의 새로운 정보
5 주요 결과

7 **전체 결과**
8 글로벌 하이라이트
13 초기 공격 벡터 및 근본 원인
14 데이터 유출 주기
15 유출 파악
17 보안 인공지능 및 자동화
20 유출 후 가격 인상
20 비즈니스 중단
21 복구 시간
23 유출 비용을 증가시키거나 감소시키는 요인
25 갈취 공격 비용
28 유출 및 규제 벌금 신고
29 데이터 보안
32 대규모 유출
33 보안 투자

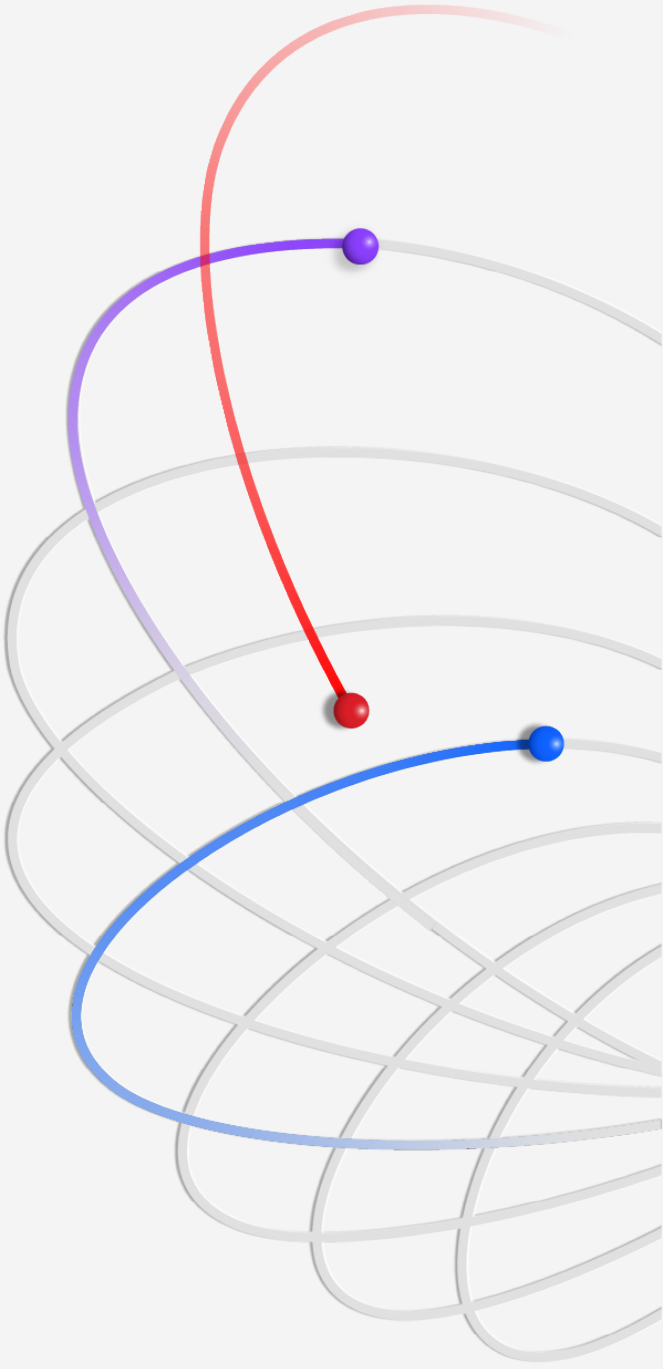
34 **데이터 유출 비용을 줄이는 데 유용한 권장 사항**
데이터 유출 비용

37일차 **조직 인구 통계**
38 지역 인구 통계
39 산업 인구 통계
40 산업 정의

41 **연구 방법론**
42 데이터 유출 비용을 계산하는 방법
43 데이터 유출 FAQ
44 연구 제한사항

45 **IBM 및 Ponemon Institute 소개**

개요



IBM의 연례 데이터 유출 비용 보고서는 IT/위험 관리/보안 부문 책임자의 전략적 의사 결정에 도움이 되도록 시기적절하고 정량화 가능한 증거를 제시합니다. 또한 위험 프로파일 및 보안 투자에 대한 관리를 개선하는 데도 유용합니다. 역대 제19호 보고서인 금년도 보고서에는 섀도 데이터(관리 대상이 아닌 데이터 소스에 상주하는 데이터)의 증가, 데이터 유출에 따른 영업 중단의 범위와 비용 등 기술적 변동으로 인한 변화가 반영되어 있습니다.

금년도 보고서에 수록된 연구는 Ponemon Institute가 독립적으로 실시하고 IBM의 후원을 통해 분석 및 발표된 것으로, 2023년 3월 ~ 2024년 2월에 데이터 유출로 피해를 입은 604개 조직을 대상으로 진행되었습니다. 연구진은 16개 국가/지역의 17개 업종에 걸친 여러 조직을 대상으로 침해 기록이 2,100~113,000건에 달하는 유출 사고들을 조사했습니다. Ponemon Institute 연구진은 현장 실태를 파악하기 위해 각 조직의 데이터 유출 사고를 직접적으로 알고 있는 보안 책임자 및 최고 경영진 3,556명을 인터뷰했습니다.

그 결과로 작성된 보고서가 바로 경영/보안 책임자가 보안 대책을 강화하고 혁신을 이행하기 위해 사용할 수 있는 벤치마크 보고서입니다. 이 보고서는 특히 생성형 AI 이니셔티브에 맞는 보안 및 보안 분야의 AI 도입을 다루고 있습니다.

금년도 보고서에는 주요 진전 사실 2가지가 기술되어 있습니다. 그중 첫 번째는, 데이터 유출 비용의 전 세계 평균치가 전년 대비 10% 증가하여 488만 달러에 육박했다는 보고입니다. 이는 팬데믹 발발 이후 가장 큰 증가폭입니다. 이러한 비용 급증을 견인한 요인은 바로 영업 중단 및 데이터 유출 이후의 고객 지원 및 복구 작업이었습니다. 각 조직에 해당 비용의 처리 방법을 질문했을 때, 절반 이상의 조직이 고객에게 비용을 전가하고 있다고 답했습니다. 이 비용을 고객에게 부담시킨다면 인플레이션으로 인한 가격 압박을 진작부터 겪고 있는 경쟁 시장에서 낭패를 볼 수 있습니다.

두 번째로, 연구진은 동일한 위험 상황에서 방어자 측에도 보안 AI 및 자동화를 적용했을 때, 경우에 따라 데이터 유출 비용이 평균 220만 달러까지 낮아지는 등 성과가 있음을 밝혀냈습니다. AI 및 자동화 솔루션 덕분에 데이터 유출과 그로 인한 피해를 파악하고 방지하는 데 필요한 기간이 단축되고 있습니다. 다시 말해서, AI 및 자동화를 도입하지 않은 방어자는 해당 솔루션을 사용하는 방어자에 비해 데이터 유출의 감지 및 방지에 필요한 시간이 더 오래 걸리고 관련 비용도 상승할 것으로 예상됩니다.

사이버 보안팀은 이 업계 전체를 통틀어 살펴보았듯이 언제나 그 인력이 부족합니다. 금년도 연구 결과에 따르면 데이터 유출을 겪은 조직의 절반 이상이 심각한 보안 인력 부족 상태에 빠져 있으며, 해당 조직 내부의 역량 격차가 전년 대비 두 자릿수까지 늘어났습니다. 위협적인 환경이 확대됨에 따라 숙련된 보안 인력의 부족도 더욱 심화되고 있습니다. 한 조직의 거의 모든 직무에 걸쳐 생성형 AI를 도입하려는 경쟁이 계속되고 있는 가운데, 전례 없는 위험과 함께 이전보다 훨씬 더 많은 압박이 사이버 보안팀에 가해질 것으로 예상됩니다.

본 보고서는 데이터 유출로 인한 잠재적 재정 피해 및 평판 손실을 줄이기 위한 인사이트와 연구 결과에 기초하는 권고안을 제시합니다.

2024년도 보고서의 새로운 정보

IBM은 해마다 새로운 기술, 참신한 전술, 최근의 사건이 반영되도록 데이터 유출 비용 보고서를 지속적으로 갱신시키고 있습니다. 금년도 연구에서 최초로 조사된 문제는 다음과 같습니다.

- 장기간 운영 중단(예: 처리 불가능한 판매 주문, 가동이 완전히 중단된 생산 시설, 비효율적인 고객 서비스)을 경험한 조직이 있는지 여부
- 관리 대상이 아닌 데이터 소스에 저장된 데이터(섀도 데이터라고도 함)가 유출된 데이터에 포함되었는지 여부
- 조직이 보안 운영의 각 4개 영역(예방, 감지, 조사, 대응)에서 활용하고 있는 AI 및 자동화의 범위
- 갈취 공격(예: 갈취/랜섬웨어 공격 또는 갈취 및 데이터 유출만 해당)의 특성
- 데이터, 시스템 또는 서비스가 유출 이전의 상태로 복구되기까지 소요된 시간
- 조직이 유출 사실을 보고하기까지 소요된 시간(유출 사실 보고가 의무로 규정된 경우)
- 랜섬웨어 공격 이후 사법 당국의 도움을 받은 조직이 공격자가 요구한 비용을 지불했는지 여부

주요 결과

본문에 기술된 주요 결과는 Ponemon Institute에서 취합한 연구 데이터에 대한 IBM의 분석 내용에 기초합니다.

488만 달러

유출로 인한 평균 총 비용
데이터 유출 비용의 평균치가 2023년의 445만 달러에서 488만 달러로 10% 급증했습니다. 이는 팬데믹 발발 이후 가장 높은 증가율입니다. 이러한 비용 증가를 견인한 요인은 바로 영업 손실 비용(예: 운영 중단 시간, 고객 상실 등) 및 데이터 유출 후 대응 비용(예: 고객 서비스 헬프 데스크 인력 충원, 고액의 규제 과징금 납부 등)의 상승이었습니다. 상기 비용들을 합산하면 총 280만 달러인데, 이는 지난 6년간의 영업 손실 및 데이터 유출 후 활동 관련 비용 합계 중에서도 최고 수준의 금액입니다.

220만 달러

예방 작업에서의 광범위한 AI 이용에 따른 비용 절감
연구 대상 조직 3곳 중 2곳이 보안 운영 기관 전체에 보안 AI 및 자동화를 보급하고 있다고 답했습니다. 이는 전년 대비 10% 증가한 수치입니다. 공격 표면 관리(ASM), 레드팀 구성, 태세 관리 등 예방 워크플로우 전반에 걸쳐 AI 및 자동화를 광범위하게 보급한 조직은 예방 워크플로우에 AI를 적용하지 않은 조직에 비해 평균 220만 달러의 데이터 유출 비용을 절감했습니다. 이 결과는 2024년도 보고서를 통해 공개된 비용 절감 사례 중 최대 규모를 자랑합니다.

26.2%

사이버 역량 부족의 심화
데이터 유출을 겪은 조직의 절반 이상이 심각한 보안 인력 부족 상태에 빠져 있습니다. 이 문제는 데이터 유출 비용이 전년 대비 26.2% 증가하면서 평균 176만 달러의 유출 비용이 더 발생한 상황을 대변합니다. 조직 5곳 중 1곳이 생성형 AI 보안 도구(생산성과 효율성을 높여 격차를 줄이는 데 유용할 것으로 기대됨)를 어떤 형태로든 사용한다고 답했지만, 이러한 역량 격차는 여전히 해결이 시급한 과제입니다.

3분의 1

섀도 데이터 관련 유출 사고의 비율
데이터 유출 사고의 35%는 섀도 데이터와 관련이 있습니다. 이는 데이터의 확산으로 인해 추적 및 보호 작업이 더욱 어려워지고 있음을 의미합니다. 섀도 데이터 도용은 데이터 유출 비용이 16% 증가한 현상과 관련이 있었습니다. 연구진이 밝혀낸 바에 따르면 여러 환경마다 데이터를 저장하는 것이 일반적인 스토리지 전략으로 입증되었는데, 이러한 원인이 데이터 유출 사고의 40%를 차지했습니다. 이러한 유출 사고는 파악 및 억제 과정에 소요되는 시간도 길어지는 것으로 나타났습니다. 반면에 퍼블릭 클라우드(25%), 온프레미스(20%) 또는 프라이빗 클라우드(15%) 등 한 가지 유형의 환경에만 저장된 데이터는 유출 빈도가 더 낮았습니다.

499만 달러

악의적인 내부자 공격의 평균 비용
다른 경로들과 비교했을 때, 악의적인 내부자 공격은 평균 499만 달러에 달하는 최고 수준의 비용을 초래했습니다. 이외에도 피해 액수가 높은 공격 경로로는 비즈니스 이메일 유출, 피싱, 소셜 엔지니어링, 자격 증명 도용 또는 훼손 등이 있었습니다. 이러한 피싱 공격 중 일부 사례에서는 생성형 AI가 공격을 실행하는 역할을 담당했을 수 있습니다. 예를 들면 영어가 모국어가 아닌 공격자라 할지라도, 생성형 AI를 사용하면 문법적으로 정확하고 조리에 맞는 피싱 메시지를 그 어느 때보다도 쉽게 작성할 수 있습니다.

46%

고객 개인 데이터 관련 유출 사고의 비율
모든 데이터 유출 사고 중 거의 절반이 납세자 식별(ID) 번호, 이메일, 전화번호, 집 주소 등 고객의 개인 식별 정보(PII)와 관련 있는 사례였습니다. 지식재산권(IP) 기록이 근소한 차이로 그 뒤를 이어 2위(전체 유출 사고의 43%)에 올랐습니다. IP 기록의 비용은 전년도 보고서에서는 기록 1건당 156달러였고, 금년도 연구 결과에서는 전년 대비 큰 폭으로 기록 1건당 173달러까지 증가했습니다.

미화 1백만 달러

랜섬웨어 공격 시 사법 당국의 도움을 받은 경우의 비용 절감
사법 당국의 개입으로 랜섬웨어 피해를 입은 사람들은 공격자에게 지불한 요구 비용을 제외하고도 데이터 유출 비용을 평균 100만 달러 가까이 낮출 수 있었습니다. 그뿐만 아니라 사법 당국이 개입함으로써 데이터 유출의 파악 및 억제에 필요한 시간을 297일에서 281일로 단축할 수도 있었습니다.

292

자격 증명 도용 관련 유출을 파악하고 방지하기까지 소요된 일수
모든 공격 경로 중에서도 도용되었거나 훼손된 자격 증명과 관련 있는 데이터 유출을 파악하고 방지하는 데 가장 오랜 시간(292일)이 소요되었습니다. 직원과 직원의 접근 권한을 이용한 유사 공격을 해결하는 데에도 긴 시간이 걸렸습니다. 그 예로 피싱 공격의 지속 기간은 평균 261일, 소셜 엔지니어링 공격의 지속 기간은 평균 257일이었습니다.

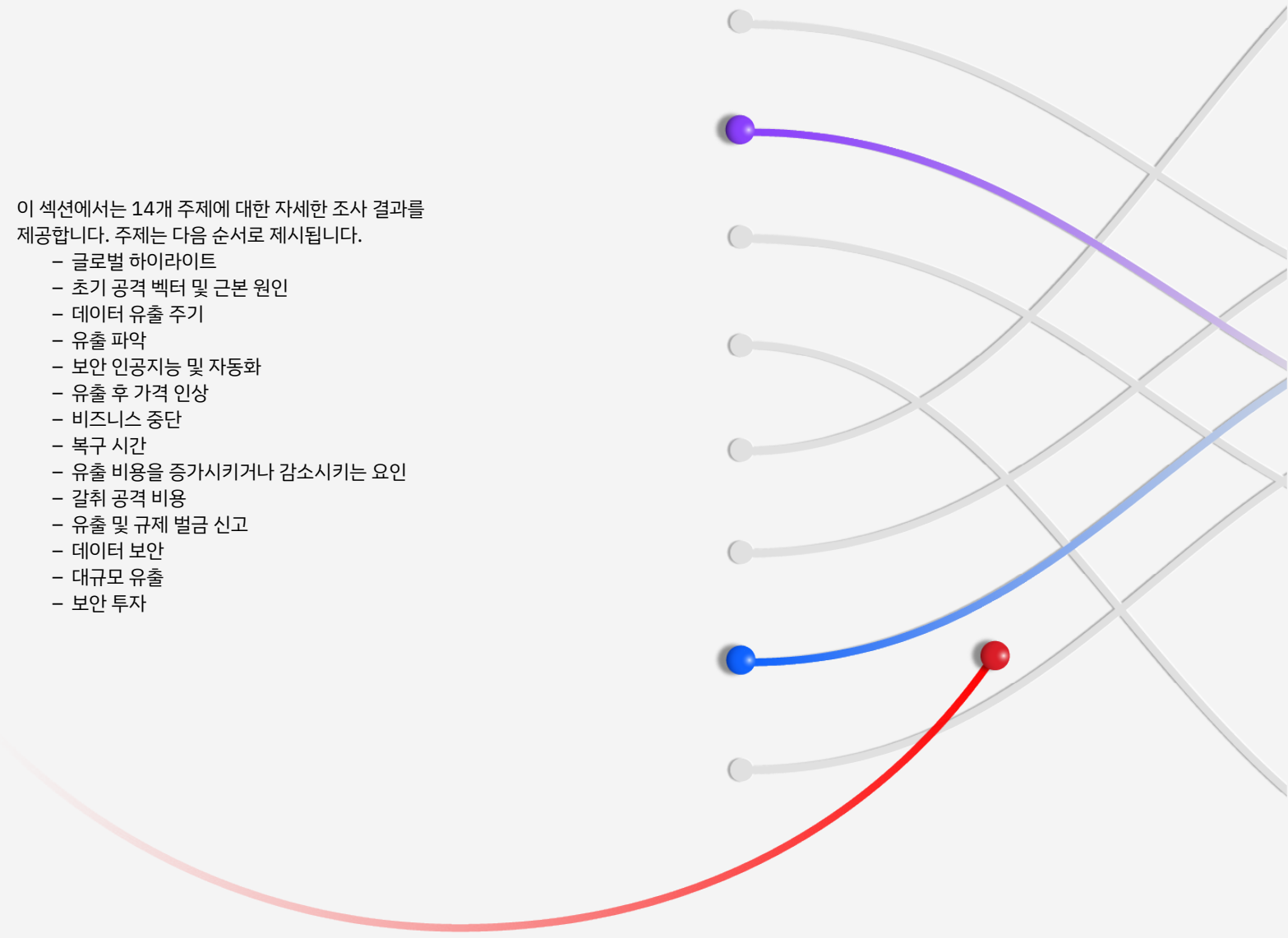
83만 달러

모든 업종을 통틀어 최고 수준인 평균 비용 증가율
공업 부문은 데이터 유출 1건당 평균 비용이 전년 대비 83만 달러 증가하면서 모든 업종 중에서도 가장 큰 폭의 증가율을 기록했습니다. 이 부문의 조직들은 운영 중단 시간에 매우 민감합니다. 따라서 앞서 설명한 비용 급증은 공업 조직이 더욱 신속하게 대응할 수 있도록 대비해야 할 필요성을 시사할 수 있습니다. 이러한 상황에서도 공업 조직이 데이터 유출을 파악하고 억제하는 데 소요된 시간은 파악에 199일, 억제에 73일로 업종별 중앙값보다 높게 나타났습니다.

전체 결과

이 섹션에서는 14개 주제에 대한 자세한 조사 결과를 제공합니다. 주제는 다음 순서로 제시됩니다.

- 글로벌 하이라이트
- 초기 공격 벡터 및 근본 원인
- 데이터 유출 주기
- 유출 파악
- 보안 인공지능 및 자동화
- 유출 후 가격 인상
- 비즈니스 중단
- 복구 시간
- 유출 비용을 증가시키거나 감소시키는 요인
- 갈취 공격 비용
- 유출 및 규제 벌금 신고
- 데이터 보안
- 대규모 유출
- 보안 투자



488만 달러

데이터 유출로 인한 글로벌 평균 비용

글로벌 하이라이트

전 세계적으로 보안 팀은 심각한 기술 부족을 겪고 있음에도 유출을 탐지하고 억제하는 데 있어 훨씬 더 나은 성과를 보입니다. 데이터 유출을 당한 조직의 절반 이상이 보안 인력 부족에 직면해 있으며, 보안 리더들은 AI와 자동화 솔루션을 활용하여 기술 격차를 메우고 있습니다. 이러한 노력에도 불구하고 유출 비용은 증가하고 있으며, 주로 비즈니스 중단과 유출 발생 후 대응과 관련된 비용이 증가하고 있습니다. 다음 섹션에서는 이러한 이슈를 비롯하여 산업, 국가, 및 지역에 걸친 문제를 살펴봄으로써 보안 리더에게 현존하는 위험에 대한 관점을 제시하고 이를 통해 배울 점을 찾아봅니다.

데이터 유출로 인한 글로벌 평균 비용

데이터 유출로 인한 전 세계 평균 비용은 1년 동안 10% 증가해 488만 달러에 달했고, 이는 팬데믹 이후 가장 큰 폭의 증가입니다. 그 중 비즈니스 중단과 유출 후 대응 조치가 연간 비용 증가 원인의 대부분을 차지했습니다 (그림 1 참조).

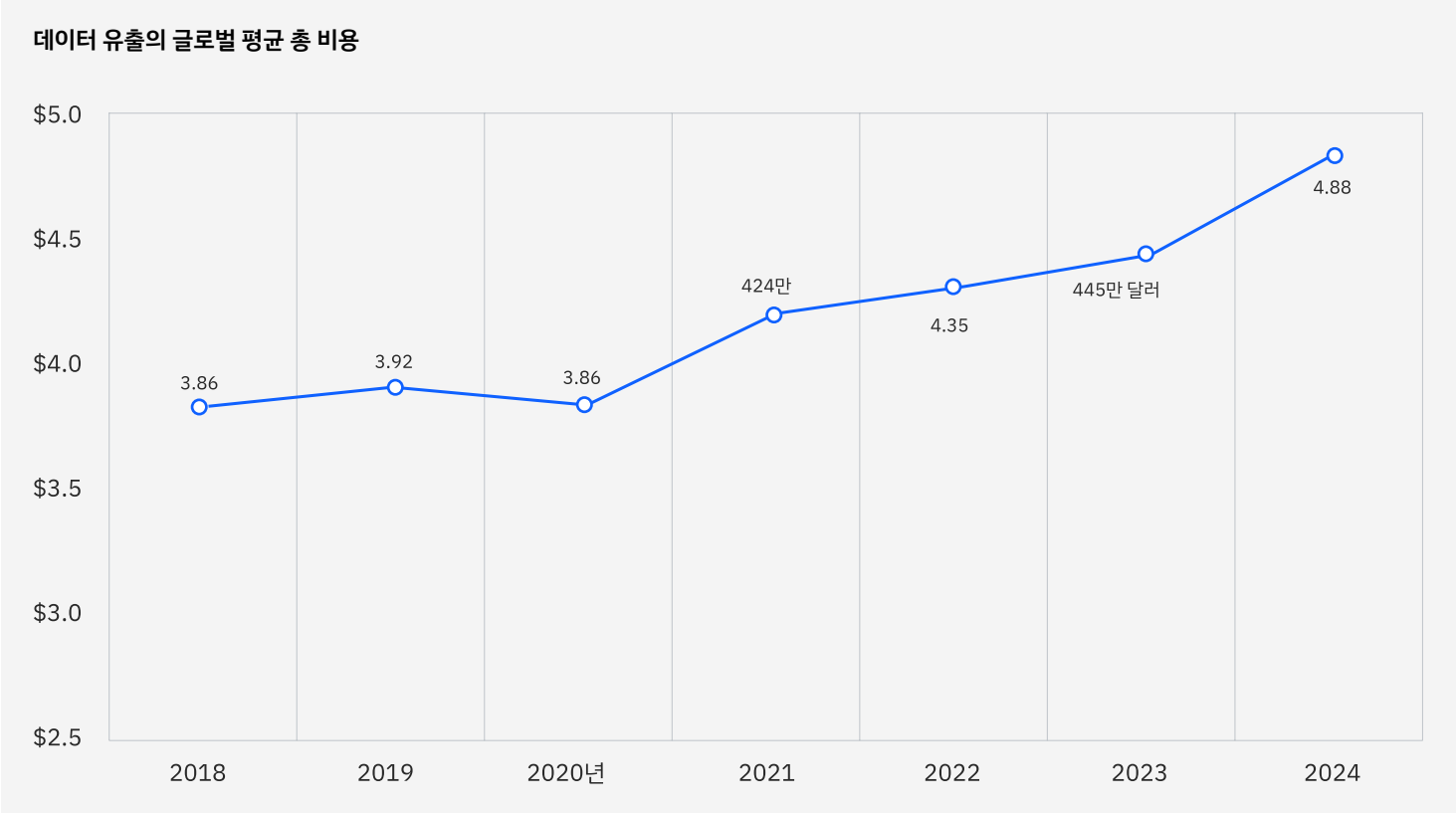


그림 1. 미화 100만 달러 단위 기재

미국이 평균 침해 비용에서 전 세계 최고를 차지
미국은 조사 대상 16개국 및 지역 중에서 14년째 평균 데이터 침해 비용이 가장 높았으며, 그 비용은 936만 달러였습니다. 이어서 중동, 독일, 이탈리아, 베네룩스가 상위 5위를 차지했습니다. 베네룩스는 벨기에, 네덜란드, 룩셈부르크 경제 연합으로 올해 조사에 새롭게 추가되었습니다. 특히 캐나다와 일본은 평균 비용이 감소한 반면, 이탈리아와 중동은 크게 증가했습니다(그림 2A 및 2B 참조).

국가 또는 지역별 데이터 유출 비용

#	국가	2024	2023
1	미국	$9.36	$9.48
2	중동	$8.75	$8.07
3	베네룩스	$5.90	—
4	독일	$5.31	$4.67
5	이탈리아	$4.73	$3.86
6	캐나다	$4.66	$5.13
7	영국	$4.53	$4.21
8	일본	$4.19	$4.52
9	프랑스	$4.17	$4.08
10	라틴 아메리카	$4.16	$3.69
11	한국	$3.62	$3.48
12	아세안	$3.23	$3.05
13	오스트레일리아	$2.78	$2.70
14	남아프리카 공화국	$2.78	$2.79
15	인도	$2.35	$2.18
16	브라질	$1.36	$1.22

그림 2A. 미화 100만 달러 단위로 측정

상위 5개 국가 및 지역의 2023년과 2024년 비교

#	비용 변경	2024	2023
1	↓	**미국** $9.36	**미국** $9.48
2	↑	**중동** $8.75	**중동** $8.07
3	↑	**베네룩스** $5.90	**캐나다** $5.13
4	↑	**독일** $5.31	**독일** $4.67
5	↑	**이탈리아** $4.73	**일본** $4.52

그림 2B. 미화 100만 달러 단위로 측정

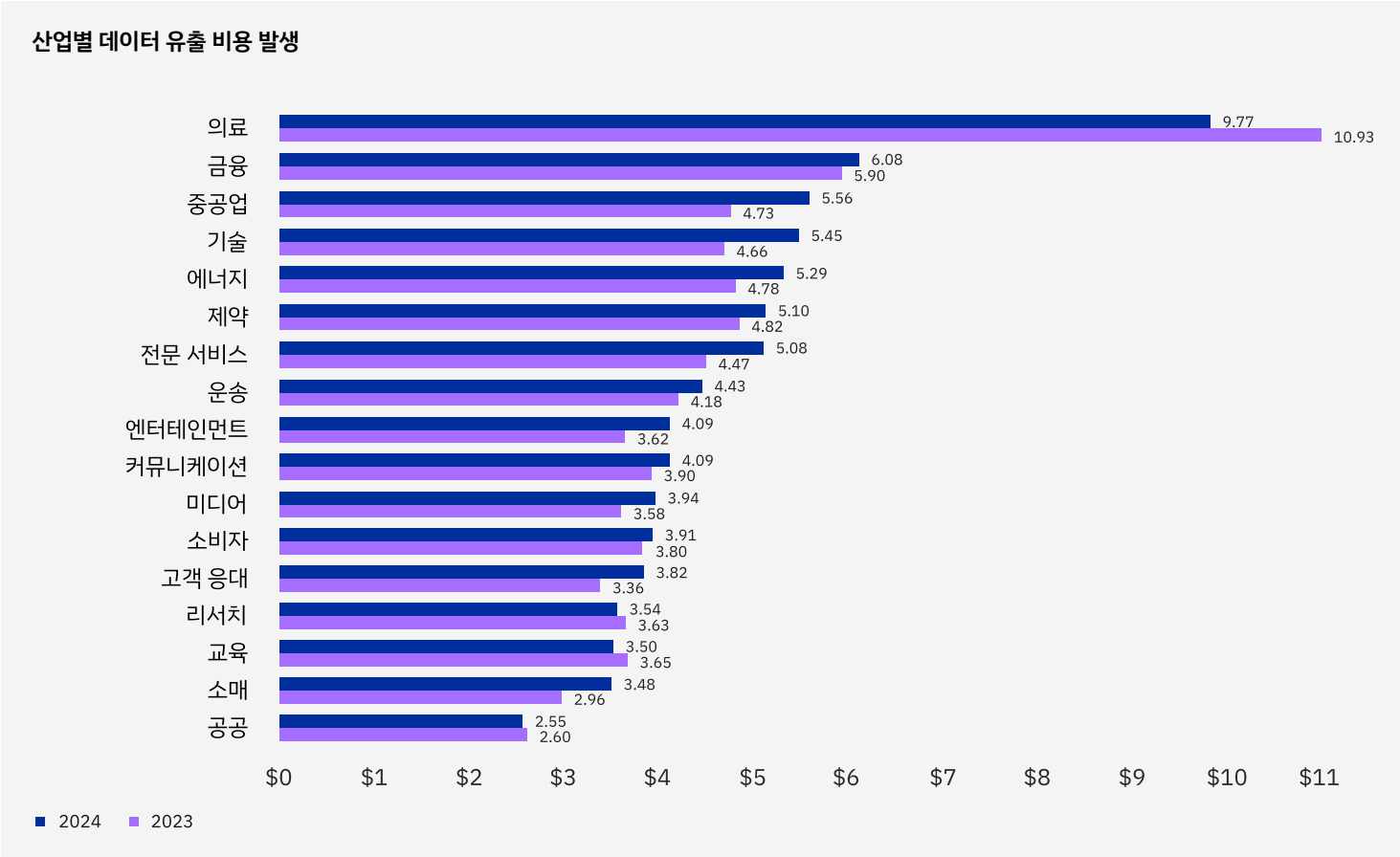


그림 3. 미화 100만 달러 단위 기재

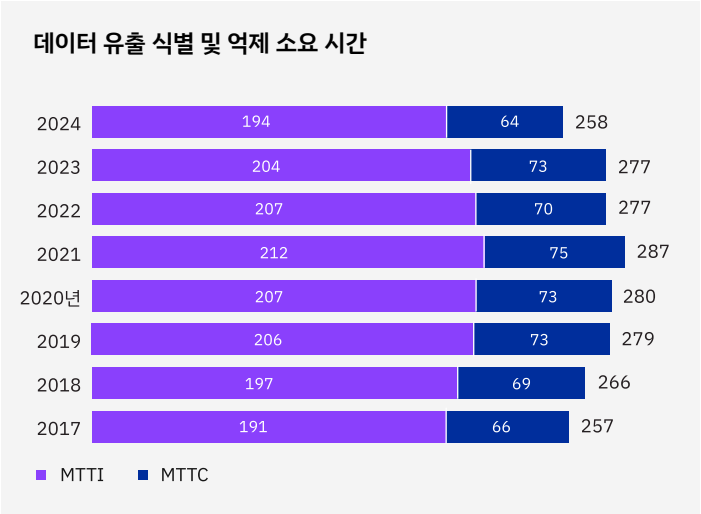


그림 4. 일 단위로 측정

또 다시 업계별 비용 1위를 차지한 의료 분야
의료 분야의 평균 유출 비용은 10.6% 감소한 977만 달러로 확인되었습니다. 그러나 이런 수치만으로는 의료 분야가 2011년부터 데이터 유출 사고로 인해 가장 큰 비용을 지출한 업계라는 현실을 벗어나기에는 역부족이었습니다. 의료 분야는 기존 기술로 인해 어려움을 겪는 경우가 많고 비즈니스 중단에 가장 취약하여 환자의 안전이 위태로워질 수 있기 때문에 공격자들의 표적이 되고 있습니다 (그림 3 참조).

유출 파악 및 억제에 드는 평균 시간 감소
방어자가 유출을 파악하고 억제하는 데 걸리는 평균 시간은 전년의 277일과 비교해 258일로 떨어져, 7년 만에 최저치를 기록했습니다. 참고로, 베네룩스는 연구에 포함된 새로운 지역으로서 영향력이 크고 평균보다 결과가 훨씬 왜곡되었기 때문에 평균 파악 시간(MTTI)과 평균 억제 시간(MTTC)의 전 세계 평균 산정에서 제외되었습니다 (그림 4 참조).

비즈니스 손실 비용 및 유출 후 대응 비용 급증
비즈니스 손실 및 유출 후 대응으로 인한 비용이 전년 대비 약 11% 증가하여 전체 유출 비용이 상당히 증가했습니다. 비즈니스 손실 비용에는 시스템 다운타임으로 인한 수익 손실과 고객 손실 및 평판 손상 비용이 포함됩니다. 유출 후 비용에는 유출로 인해 영향을 받은 고객을 위한 콜센터 및 신용 모니터링 서비스 구축 비용과 규제 벌금 납부 비용이 포함됩니다(그림 5 참조).

데이터 유출의 네 가지 구성 요소에 따른 평균 비용

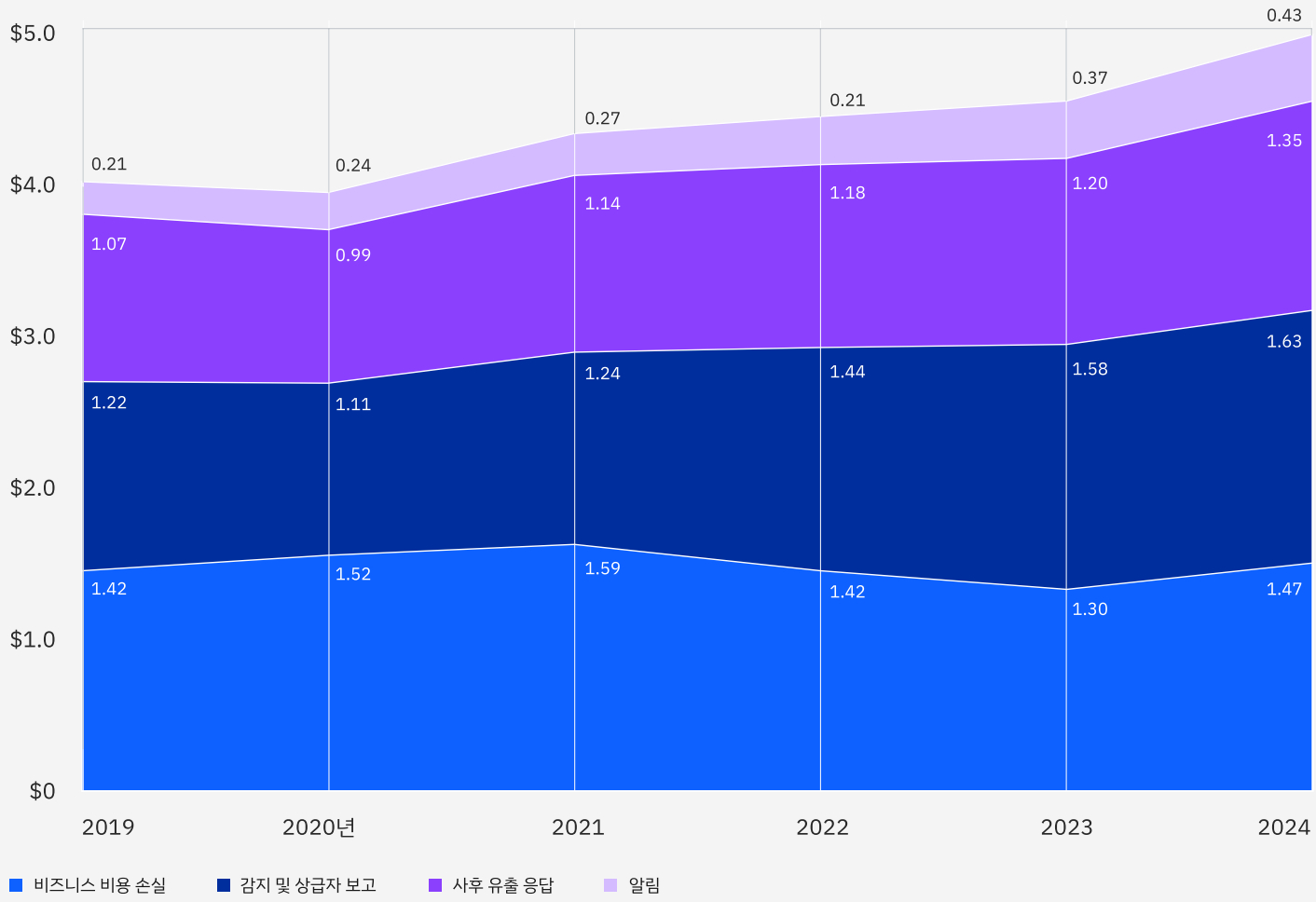


그림 5. 미화 100만 달러 단위로 측정

대부분의 유출 사고는 고객 개인 식별 정보와 관련
도난 또는 유출된 데이터의 가장 일반적인 유형은 고객 개인 식별 정보로 46%에 달했습니다. 개인 식별 정보로는 납세자 번호, 이메일, 집 주소 등이 있으며 이는 신원 도용, 신용 카드 사기에 사용될 수 있습니다.
모든 도난 기록 유형에 관한 전 세계 평균 비용은 169달러로 최고치를 기록했으며, 직원 개인 식별 정보가 피해 비용이 가장 컸습니다 (그림 6A 및 6B 참조).

유출된 데이터 유형별 비율

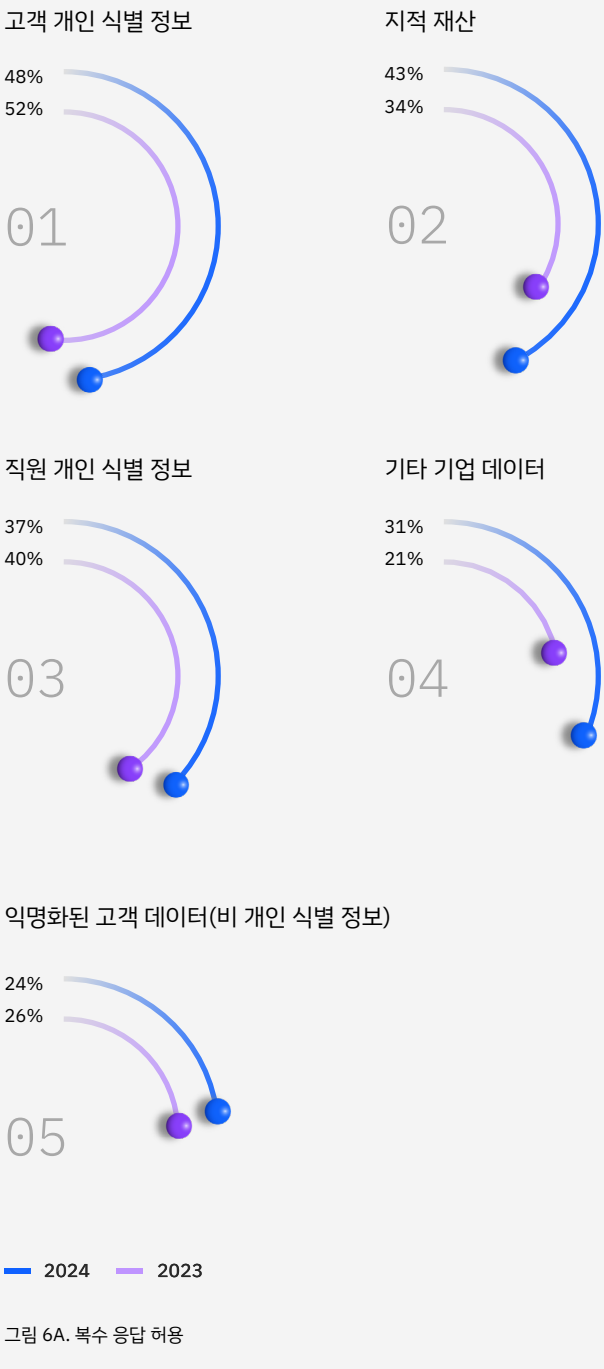


그림 6A. 복수 응답 허용

유출된 기록 유형별
기록당 데이터 유출 비용

그림 6B. 미화 100만 달러 단위로 측정

미화 481만 달러

공격자가 유출된 자격 증명을 사용했을 때 발생한 평균 유출 비용으로, 연구 대상 유출 사례의 16%에서 발생했습니다.

초기 공격 벡터 및 근본 원인

2년 연속 피싱과 도난 또는 손상된 자격 증명이 가장 많이 발생한 공격 벡터 2위를 차지했습니다. 또한 이 둘 다 가장 비용이 많이 드는 인시던트 유형 상위 4위 안에 들었습니다. 이 연구에서는 가장 일반적인 근본 원인을 파악하는 것 외에도 각 범주의 유출로 인한 평균 비용과 해당 유출을 파악하고 억제하는 데 드는 평균 시간 또한 비교했습니다.

손상된 자격 증명이 초기 공격 벡터 1위 차지

공격자가 손상된 자격 증명을 사용하여 이득을 취하는 것이 유출 사고의 16%를 차지했습니다. 손상된 자격 증명을 사용한 공격은 조직에 큰 비용을 초래할 수 있으며, 유출당 평균 481만 달러의 비용이 발생합니다. 피싱은 공격 벡터의 15%로 근소한 차이로 2위를 차지했지만, 결국에는 488만 달러로 더 큰 비용이 발생했습니다. 악의적인 내부자 공격이 499만 달러로 가장 큰 비용이 발생했지만, 전체 유출 경로의 7%에 불과했습니다 (그림 7 참조).

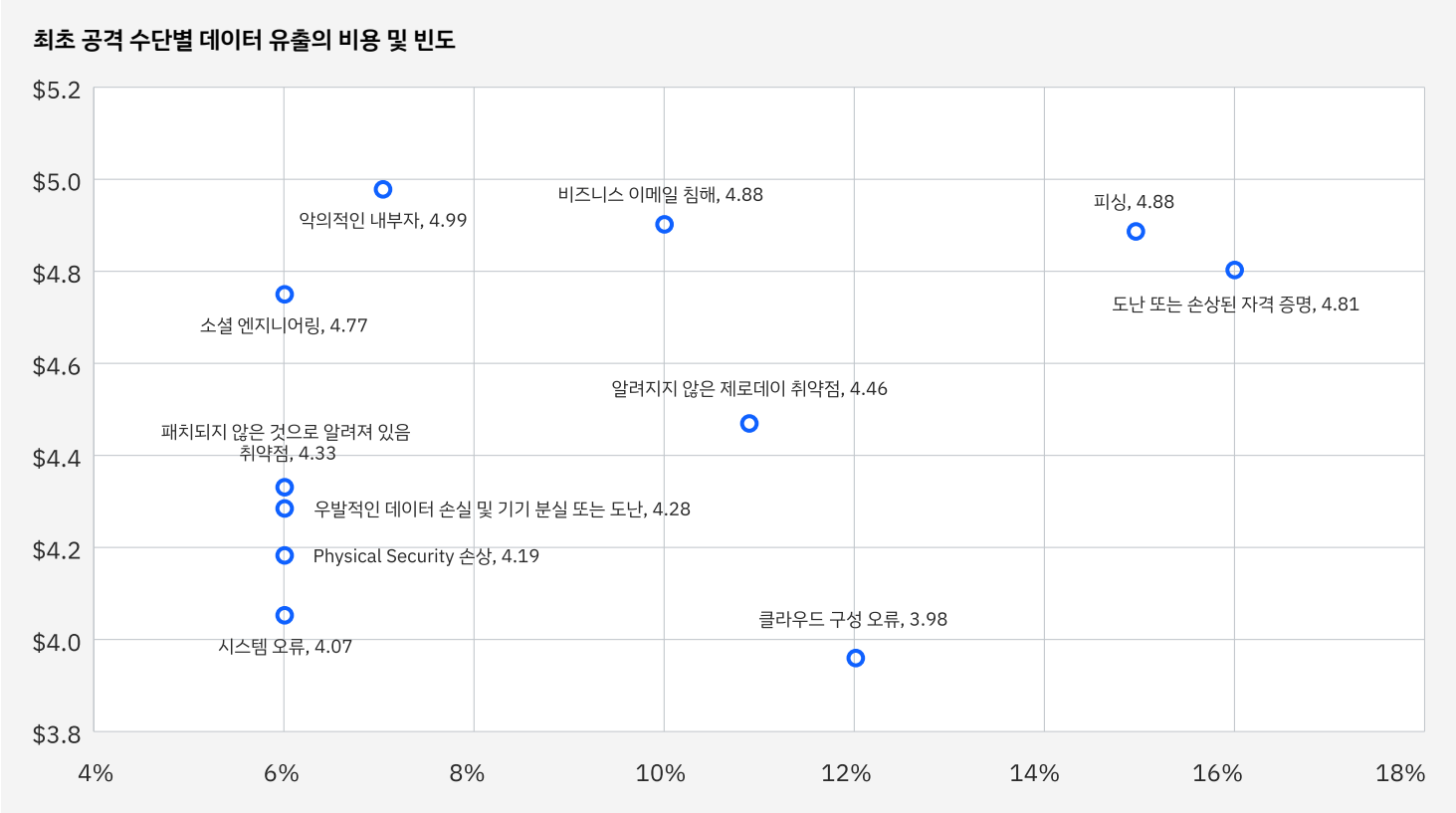


그림 7. 미화 100만 달러 단위로 측정, 전체 유출 중 비율

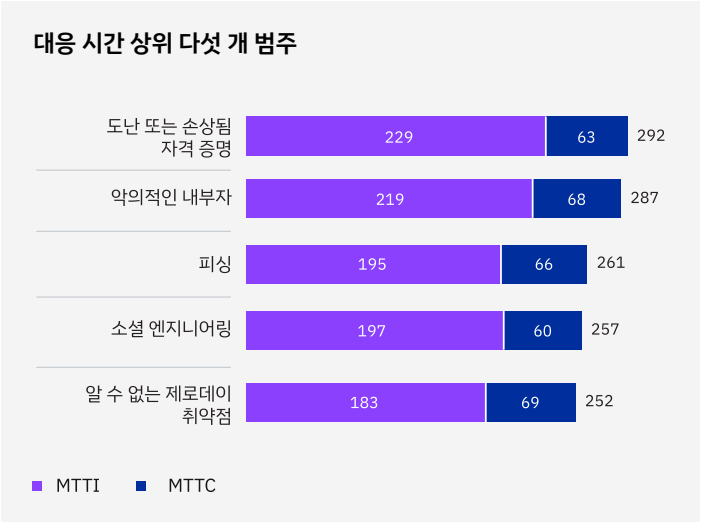


그림 8. 일 단위로 측정

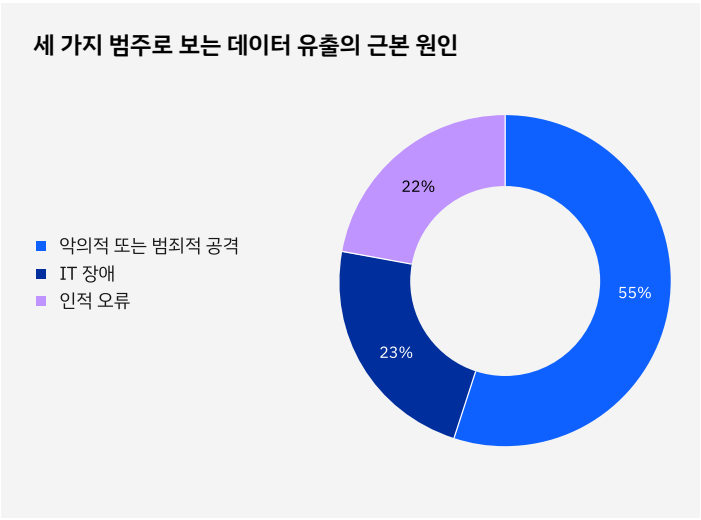


그림 9.

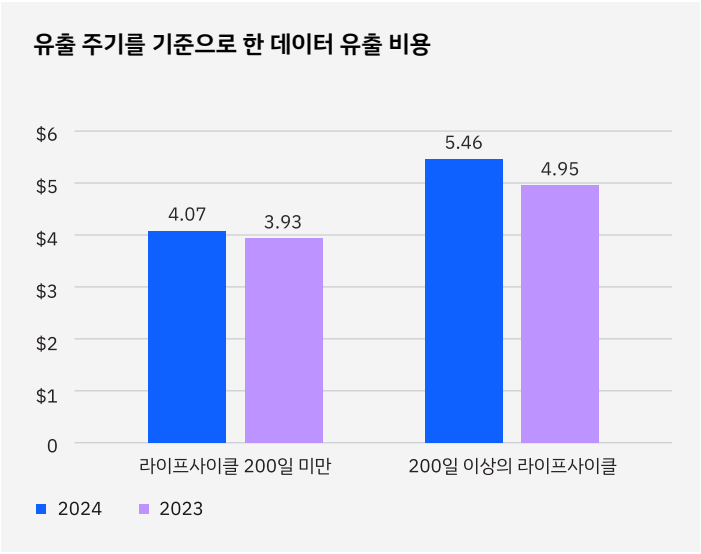


그림 10. 미화 100만 달러 단위 기재

자격 증명 기반 공격은 파악 및 억제에 더 오랜 시간 소요
자격 증명은 도난당했든 악의적인 내부자가 사용했든 간에, 공격을 파악하고 억제하는 데 걸리는 시간이 증가해 평균적으로 각각 292일, 287일이 소요되었습니다. 방어자는 네트워크에서 합법적인 사용자 활동과 악의적인 사용자 활동을 구분해야 했기 때문에 위협을 식별하기가 더 어려워졌습니다. 반면, 제로데이 취약점을 사용한 공격이 억제하는 데 가장 많은 시간이 소요되었습니다 (그림 8 참조).

전체 유출 사고의 거의 절반이 IT 장애 또는 인적 오류로 인해 발생
외부 공격자 또는 내부 범죄자에 의한 악의적 공격이 전체 데이터 유출의 55%를 차지했습니다. 이러한 유출이 우려되는 만큼, 나머지 23%는 IT 장애로 인한 것이며 22%는 인적 오류로 인한 것임을 기억하는 것도 중요합니다 (그림 9 참조).

데이터 유출 주기

2023년과 2024년 조사에 따르면 데이터 유출에 있어 시간은 곧 돈이며 유출 라이프사이클이 길어질수록 더 큰 비용이 발생했습니다. 전체 유출 라이프사이클은 유출을 파악하고 억제하는 데 걸리는 평균 일수를 합한 것입니다. 두 조사 보고서 모두에서 전체 유출 라이프사이클이 200일 미만인 데이터 유출의 평균 비용과 전체 라이프사이클이 200일을 초과한 유출의 평균 비용을 비교했습니다.

라이프사이클이 길수록 비용 증가
올해 보고서에서 연구진은 라이프사이클이 200일 미만인 데이터 유출에 비해 라이프사이클이 200일을 초과하는 유출에 따른 비용이 546만 달러로 가장 높았다는 사실을 발견했습니다. 이러한 결과는 전년도의 연구 결과와 일치합니다. 특히 작년에 비해 올해에, 더 길어진 데이터 유출 라이프사이클의 비용이 10.3% 증가했으며 더 짧아진 라이프사이클 비용도 증가했지만, 3.6%로 그 폭은 더 작았습니다 (그림 10 참조).

유출 파악

데이터 유출을 억제하려면 먼저 이를 식별해야 합니다. 누가, 얼마나 빨리 식별하느냐에 따라 데이터 유출로 인한 비용이 달라집니다. 올해에는 자체 툴을 사용하는 보안 팀이 이 영역에서 성능을 개선한 것으로 확인되었습니다. 다른 경우에는 보안 연구원, 사법 당국, 컨설턴트와 같은 선의의 제3자 또는 공격자에 의해 유출이 파악되었습니다.

보안 팀이 대부분의 유출 파악

보안 팀과 보안 팀의 툴을 통해 유출을 탐지한 비율은 42%로, 선의의 제3자(34%)나 공격자(24%)보다 훨씬 더 많이 탐지했습니다. 이 수치는 보안 팀이 유출을 발견한 비율이 3분의 1에 불과했던 2023년 보고서와 비교해 개선된 수치입니다. 이러한 변화를 통해 보안 팀이 탐지 속도를 높일 수 있었다는 것을 알 수 있습니다(그림 11 참조).

유출은 어떻게 확인되었나요?

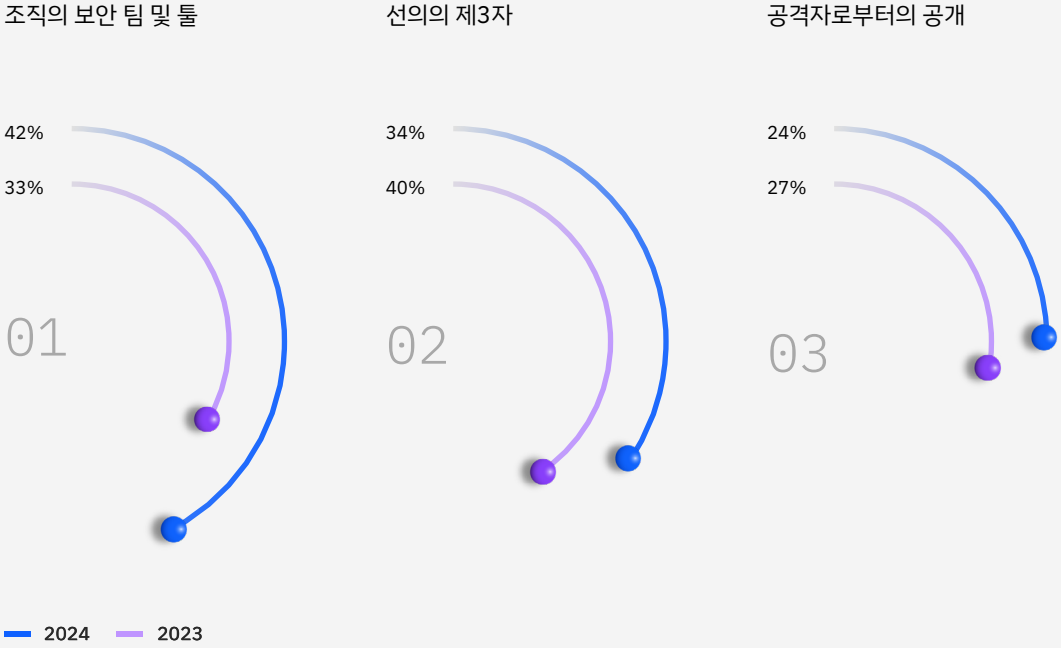


그림 11. 단독 응답만 허용

미화 553만 달러

공격자에 의해 유출이 공개되었을 때의 평균 유출 비용입니다.

공격자가 공개한 유출로 인한 비용 증가
공격자가 유출 사실을 공개할 때쯤이면, 이미 목적을 달성하고 상당한 피해를 끼친 후일 가능성이 높기 때문에 유출로 인한 전체 비용이 증가합니다. 공격자가 유출 사실을 공개했을 때 평균 비용은 553만 달러였습니다. 반면 보안 팀이 유출을 파악한 경우 평균 비용은 455만 달러였습니다 (그림 12 참조).

더 빠른 유출 파악과 억제
보고서에 따르면 유출을 발견하는 방식과 관계없이 2024년에 조직은 전년보다 평균적으로 더 빨리 유출 사실을 파악하고 억제했습니다. 보고서의 다음 섹션에서 살펴볼 수 있듯이, 이러한 가속화는 AI와 자동화 사용 덕분인 것으로 보입니다 (그림 13 참조).

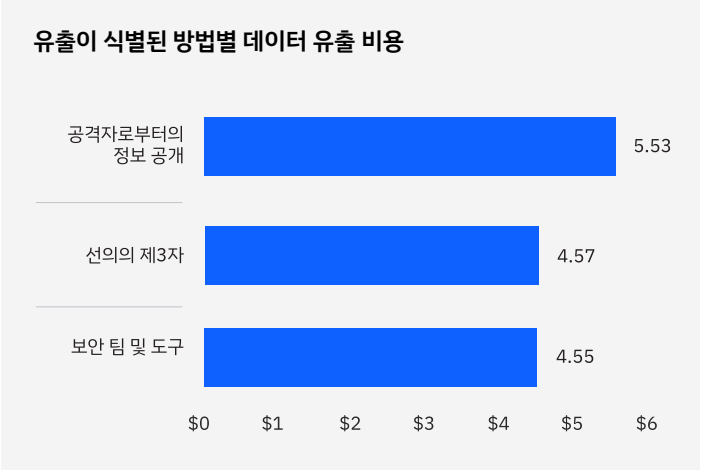


그림 12. 미화 100만 달러로 측정

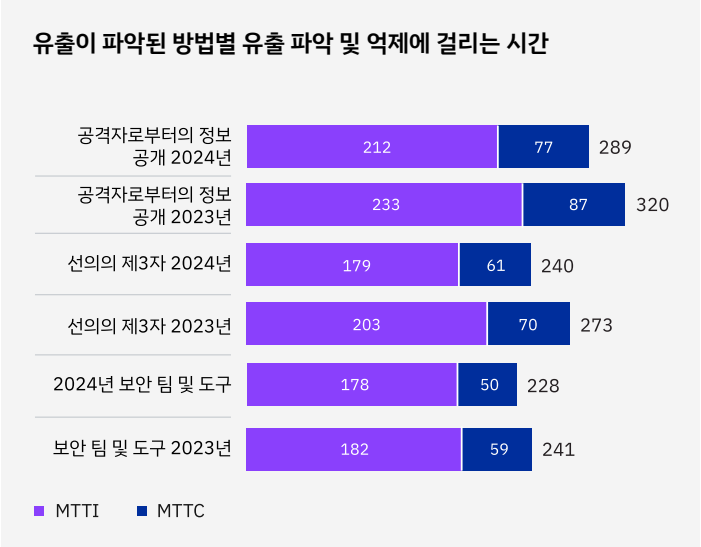


그림 13. 일 단위

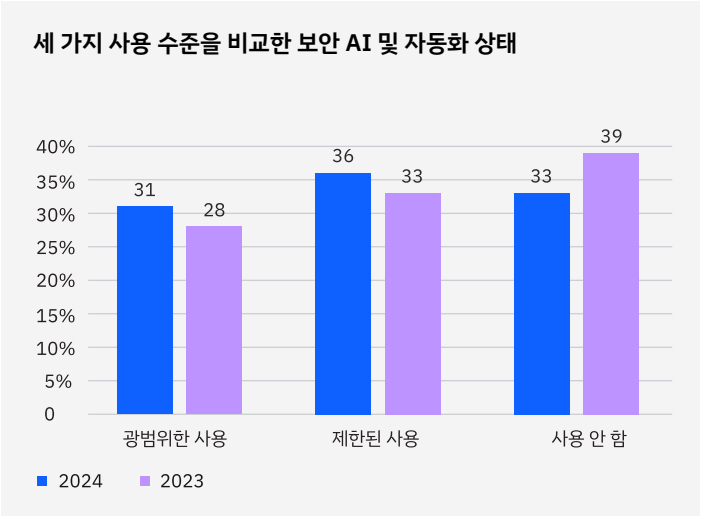


그림 14. 사용 수준당 조직의 비율

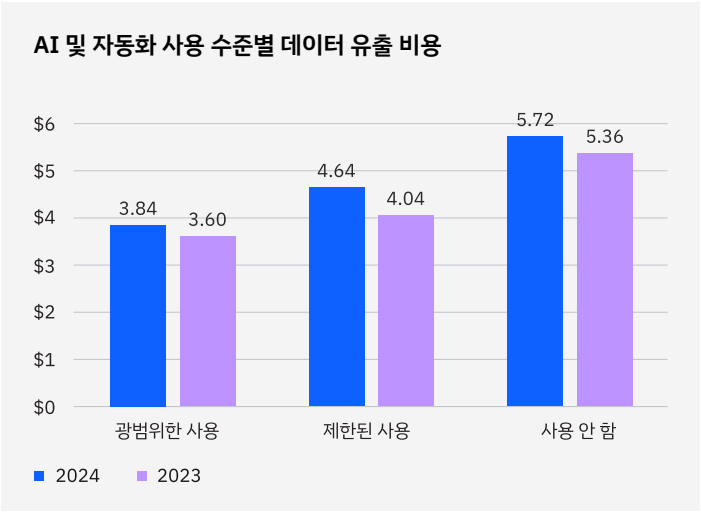


그림 15. 미화 100만 달러 단위 기재

보안 인공지능 및 자동화

AI와 자동화가 사이버 보안의 세계를 변화시키고 있습니다. 이러한 기술은 악의적인 공격자가 대규모로 공격을 생성하고 시작하는 것을 그 어느 때보다 쉽게 만들고, 방어자에게는 위협을 빠르게 파악하고 해당 위협에 대한 대응을 자동화할 수 있는 새로운 도구를 제공합니다. 올해 보고서에서는 이러한 기술이 유출 파악과 억제 및 비용 절감 작업을 더욱 빠르게 촉진하는 것으로 나타났습니다.

AI 및 자동화 사용 증가

보안 AI와 자동화를 광범위하게 사용하는 조직의 수는 작년 28%에서 올해 31%로 증가했습니다. 3% 포인트 차이이지만, 이는 사용량이 10.7% 증가한 것을 의미합니다. AI와 자동화를 제한적으로 사용하는 조직의 비율도 33%에서 36%로, 9.1% 증가했습니다 (그림 14 참조).

더 많은 AI 및 자동화를 통한 유출 비용 절감

더 많은 조직이 AI와 자동화를 사용하여 유출로 인한 평균 비용을 절감했습니다. 이러한 상관관계는 매우 주목할 만한 것으로 올해 보고서의 주요 결과입니다. AI와 자동화를 사용하지 않는 조직에 발생하는 평균 비용은 572만 달러지만, AI와 자동화를 광범위하게 사용하는 조직에 발생하는 평균 비용은 384만 달러로, 188만 달러가 절감되었습니다 (그림 15 참조).

27%

네 가지 보안 범주에 걸쳐 AI 및 자동화를 사용한 조직 비율

더 많은 AI 사용으로 더 빠른 유출 파악과 억제
보안 AI와 자동화를 광범위하게 사용하는 조직은 이러한 기술을 전혀 사용하지 않는 조직에 비해 데이터 유출 파악 및 억제에 걸리는 시간을 평균적으로 거의 100일 단축했습니다 (그림 16 참조).

AI 및 자동화를 여러 기능에 고르게 적용한 보안 팀
AI와 자동화를 광범위하게 사용한다고 답한 조직 중 약 27%가 예방, 탐지, 조사, 대응 등 각 범주에서 AI를 광범위하게 사용한다고 했습니다. 약 40%는 AI 기술을 어느 정도 사용한다고 답했습니다 (그림 17 참조).

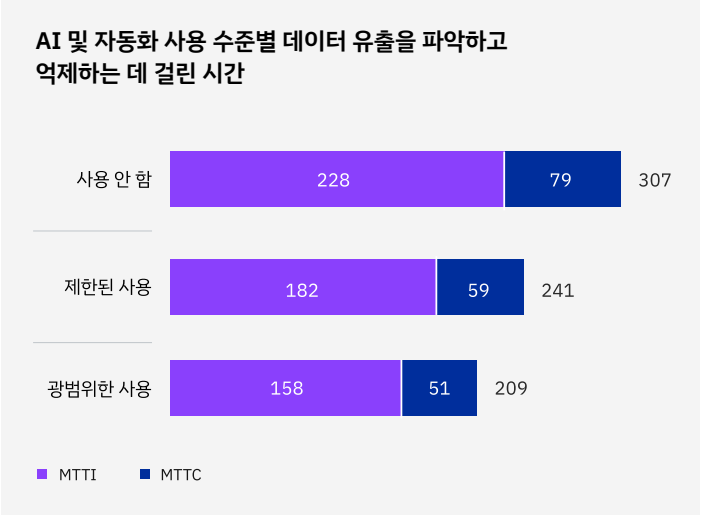


그림 16. 일 단위

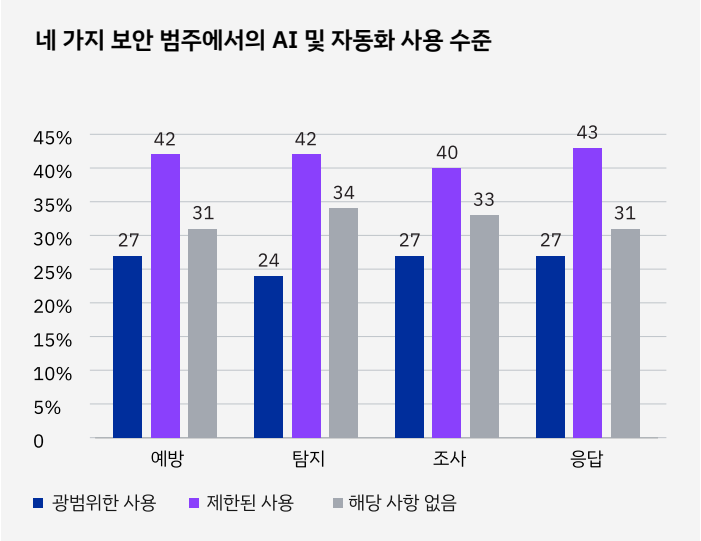


그림 17. AI 및 자동화를 광범위하게 사용한다고 보고한 응답자(차트 14 참조)

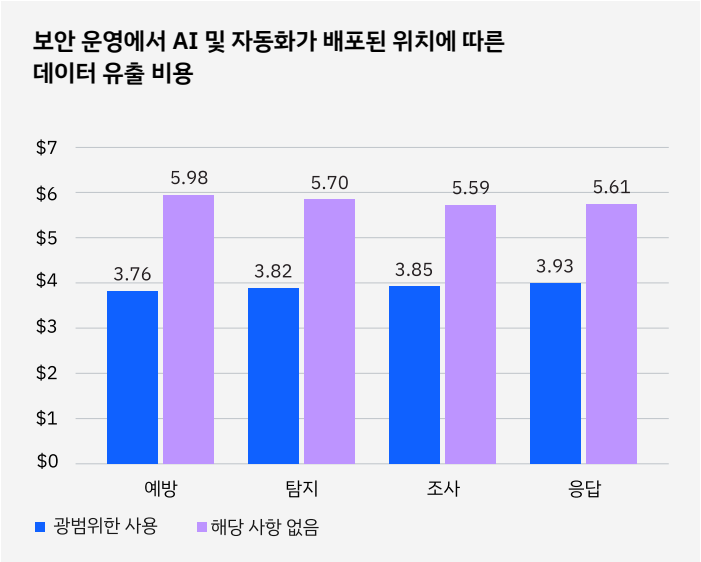


그림 18. AI 및 자동화를 광범위하게 사용한다고 보고한 조직, 미화 100만 달러 단위로 측정(차트 14 참조)

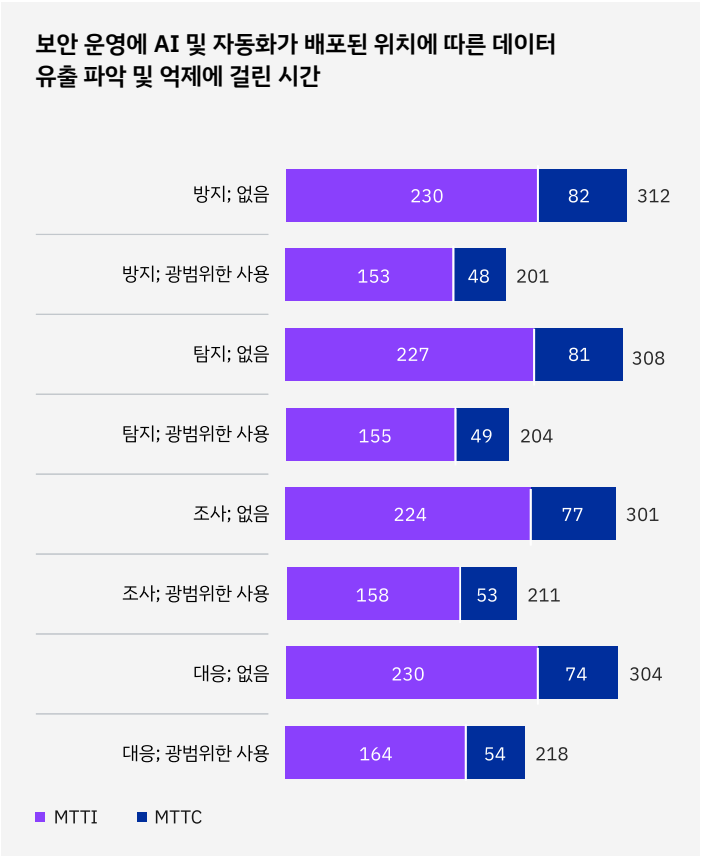


그림 19. AI 및 자동화를 광범위하게 사용한다고 보고한 조직, 미화 100만 달러 단위로 측정(차트 14 참조)

광범위한 AI 및 자동화 사용으로 비용 절감

보안의 각 네 가지 영역에서 AI와 자동화가 광범위하게 사용되었을 때, 이 영역에서 이러한 기술을 사용하지 않은 조직에 비해 유출로 인해 드는 평균 비용이 크게 절감되었습니다. 예를 들어, 조직이 예방을 위해 AI와 자동화를 광범위하게 사용했을 때, 유출로 인한 평균 비용은 376만 달러였습니다. 반면, 이러한 도구를 예방 조치에 사용하지 않은 조직은 598만 달러의 비용이 발생해 45.6%의 차이를 보였습니다 (그림 18 참조).

AI와 자동화를 통해 유출 파악 및 억제에 드는 시간 단축

AI와 자동화가 적용된 모든 곳에서 유출 파악과 억제 작업이 가속화되었습니다. 예방, 탐지, 조사, 대응 등 모든 보안 기능에 AI와 자동화를 광범위하게 사용한 경우 데이터 유출에 대한 평균 MTTI와 MTTC가 대응의 경우 33%, 예방의 경우 43% 단축되었습니다 (그림 19 참조).

70%

유출로 인해 중대하거나 매우 중대한 중단을 경험한 조직의 비율

유출 후 가격 인상

데이터 유출은 그 특성상 비용이 많이 듭니다. 조직이 수백만 달러의 비용을 부담해야 하는 상황에 부닥치면 다른 곳에서 그 비용을 만회하고자 할 수 있습니다. 이를 위한 한 가지 방법은 가격 인상을 통해 고객에게 비용을 전가하는 것인데, 이러한 현상이 점점 증가하는 추세입니다. 이미 가격 압박을 직면한 시장에서 가격 인상은 위험할 수 있습니다.

유출 비용을 고객에게 전가하는 조직

대부분의 조직이 데이터 유출 후 상품과 서비스 가격을 인상하여 고객에게 비용을 전가할 것이라고 답했습니다. 이렇게 할 계획이라고 답한 조직의 비율은 작년 57%에서 올해 63%로 10.5% 증가했습니다 (그림 20 참조).

비즈니스 중단

비즈니스는 데이터를 기반으로 운영됩니다. 데이터가 유출되면 비즈니스가 중단됩니다. 이러한 중단은 일부 시스템에만 영향을 미치는 소규모 유출부터 장기간 조직 전체에 영향을 미치는 운영 중단에 이르기까지 다양합니다. 이번 연구에서는 이러한 중단이 얼마나 경미하거나 심각한지, 또한 중단의 심각성이 데이터 유출 비용과 어떤 상관관계가 있는지 조사했습니다.

상당한 비즈니스 중단

올해 연구에 참여한 조직의 70%가 유출로 인해 심각하거나 매우 심각한 운영 중단을 경험했습니다. 단 1%만이 운영 중단 수준이 심각하지 않았다고 답했습니다(그림 21 참조).

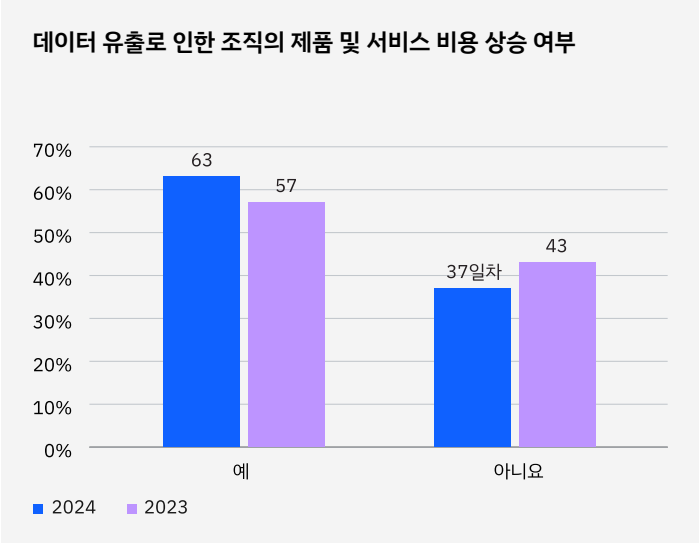


그림 20. 모든 조직의 비율

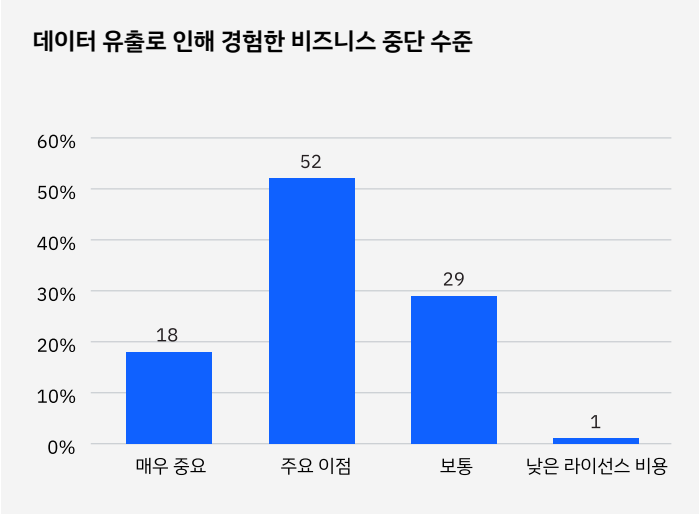


그림 21. 단독 응답만 허용

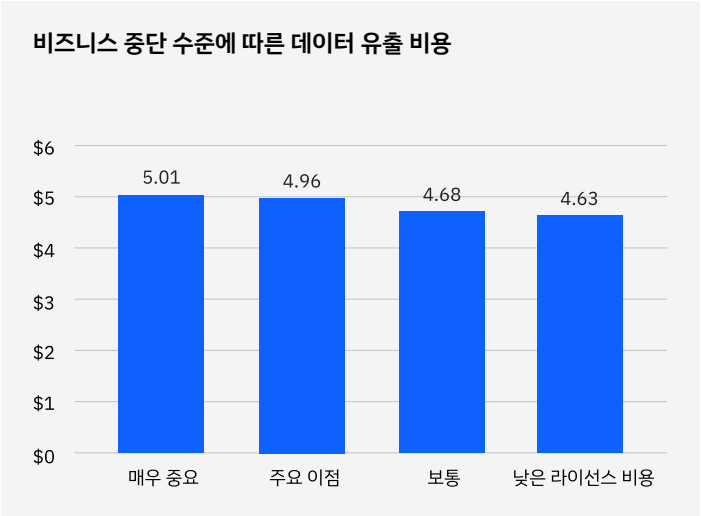


그림 22. 미화 100만 달러 단위 기재

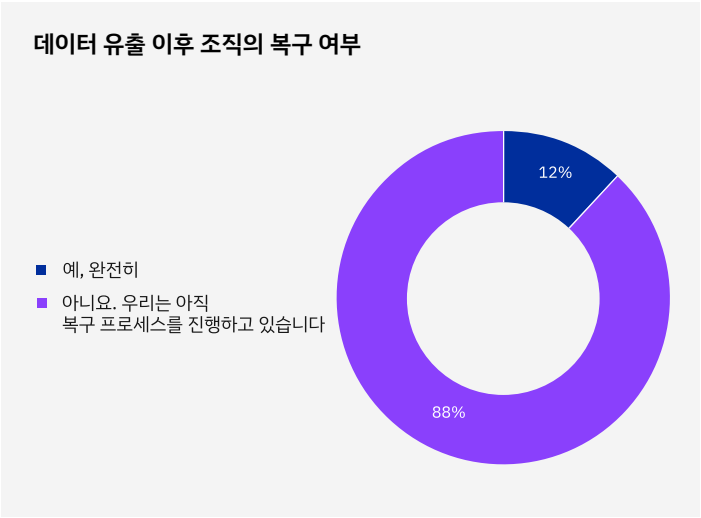


그림 23. 유출을 겪은 모든 조직의 비율

운영 중단으로 인한 평균 유출 비용 증가
비즈니스 중단이 심각할수록 평균 유출 비용이 더 컸습니다. 심각하지 않은 수준의 운영 중단을 보고한 조직도 평균 데이터 유출 비용이 463만 달러나 발생했습니다. 매우 심각한 운영 중단을 보고한 조직의 경우 발생한 평균 비용이 501만 달러로 7.9% 더 높았습니다 (그림 22 참조).

복구 시간

유출이 억제된 후에도 복구 작업은 계속됩니다. 이 연구에서 복구란 다음을 의미합니다.

- 유출의 영향을 받은 영역의 비즈니스 운영이 정상으로 돌아옴
- 조직이 벌금 납부 등 규정 준수 의무를 충족함
- 고객 신뢰와 직원 신뢰가 회복됨
- 향후 데이터 유출을 방지하기 위해 조직이 통제권, 기술 및 전문 지식을 갖추고 있음

고객 신뢰 회복과 같은 작업의 대부분은 기술 그 이상의 요소와 관련이 있습니다. 대부분의 조직에서 복구 작업은 수 개월이 걸릴 수 있습니다.

낮은 유출 복구율
올해 보고서에서 설문 조사에 참여한 조직 중 12%만이 데이터 유출 사고를 완전히 복구했다고 답했습니다. 대부분의 조직은 아직 복구 작업 중이라고 답했습니다 (그림 23 참조).

완전 복구에 100일 이상 소요
완전히 복구한 조직 중 3/4 이상이 복구에 100일 이상 걸렸다고 답했습니다. 복구는 오랜 시간이 걸리는 과정입니다. 완전히 복구한 조직의 약 1/3이 복구하는 데 150일 이상 걸렸다고 답했습니다. 완전히 복구한 조직 중 3%에 해당하는 소수만이 50일 이내에 복구했다고 답했습니다 (그림 24 참조).

데이터 유출 복구에 걸리는 평균 시간

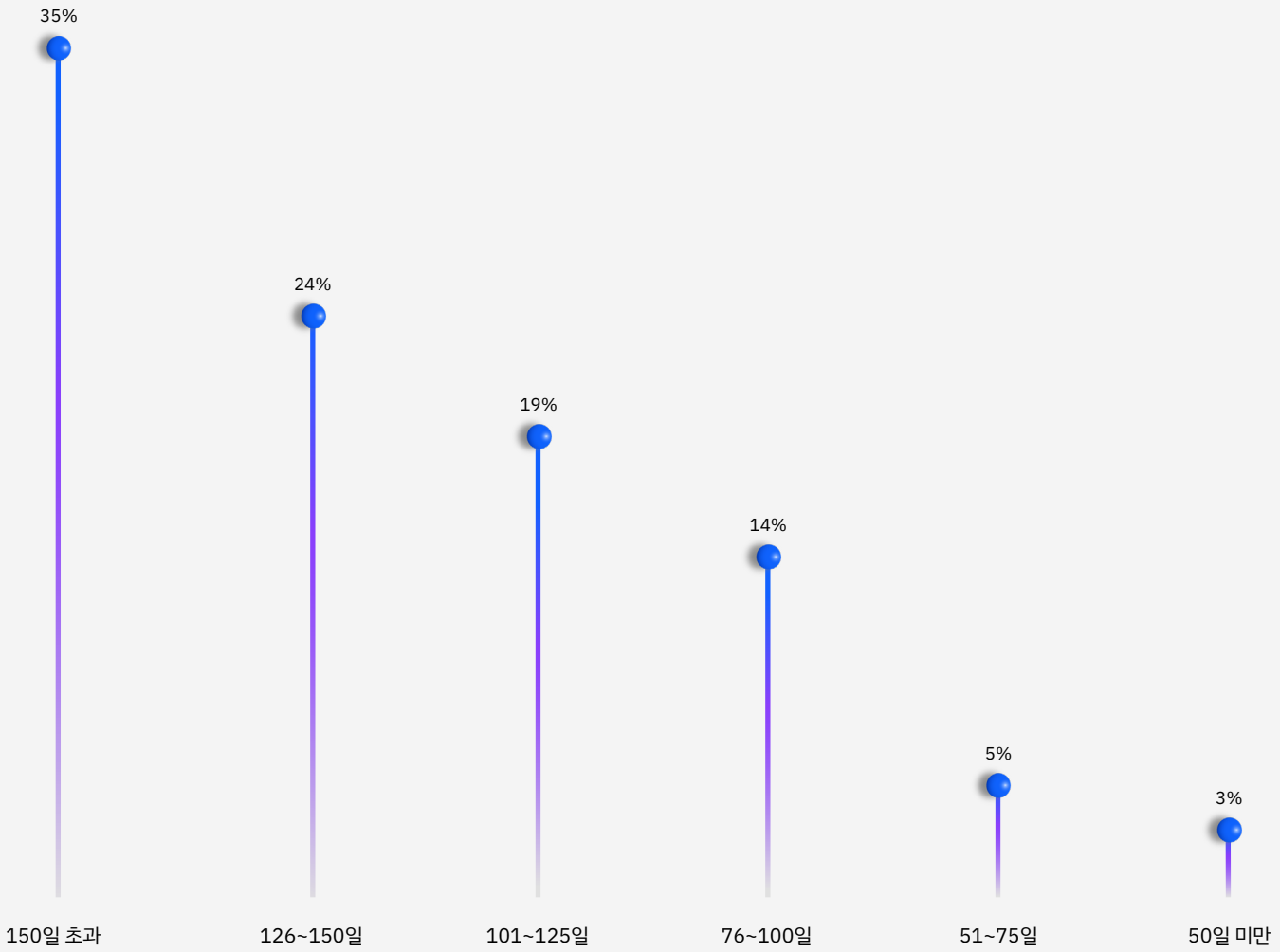


그림 24. 인시던트로부터 완전히 복구되었다고 보고한 조직, 일 단위로 측정(차트 23 참조)

그림 25. 평균 유출 비용 488만 달러와의 비용 차이(미화로 측정)

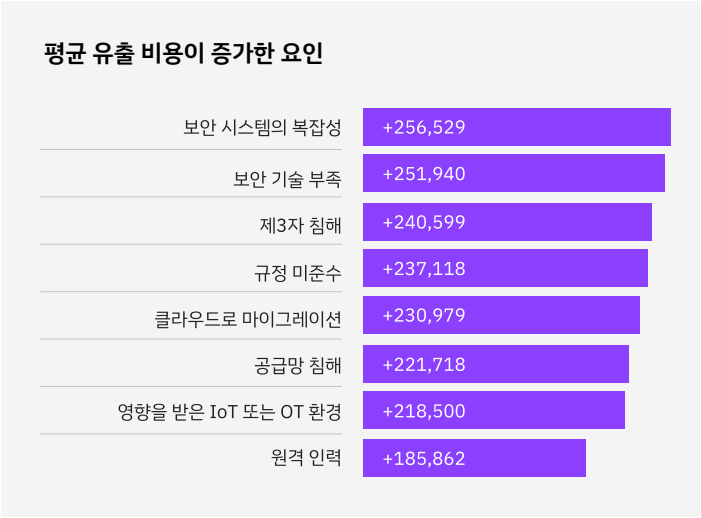


그림 26. 평균 유출 비용 488만 달러와의 비용 차이(미화로 측정)

평균 유출 비용을 감소 또는 증가시킨 요인

비용을 분석할 때에는 어떤 기술 또는 이벤트가 비용을 낮추거나 높이는지 파악하는 것이 유용합니다. 한 가지 변함없는 사실이 발견되었는데, 바로 AI와 자동화는 비용을 낮추지만, 심각한 사이버 기술 부족은 비용을 높인다는 사실입니다. 이 분석에서는 28가지의 기여 요인을 살펴보았습니다. 각 요인의 영향을 전 세계 평균과 비교하여 개별적으로 조사했습니다. 그런 다음 평균 데이터 유출 비용을 증폭하거나 완화하는 것으로 밝혀진 상위 세 가지의 요인을 살펴보았습니다.

주요 비용 절감 요인

이 분석에서 평균 데이터 유출 비용을 줄이는 가장 큰 요인은 직원 교육과 AI 및 머신 러닝 인사이트의 사용이었습니다. 직원 교육은 특히 피싱 공격을 탐지하고 막기 위한 사이버 방어 전략의 변함없는 필수 요소입니다. AI와 머신 러닝 인사이트가 근소한 차이로 2위를 차지했습니다 (그림 25 참조).

주요 비용 증가 요인

이 분석에서 유출 비용을 증폭시킨 상위 세 가지 요인은 보안 시스템 복잡성, 보안 기술 부족, 공급망 유출을 포함한 서드파티 유출이었습니다 (그림 26 참조).

574만 달러

심각한 보안 기술 부족을 겪고 있는 조직의 평균 유출 비용

주요 비용 증폭 요인의 높은 수준과 낮은 수준 비교
심각한 수준의 보안 기술 부족을 겪는 조직의 평균 유출 비용은 574만 달러로, 기술 부족 수준이 심각하지 않은 조직의 평균 유출 비용인 398만 달러보다 높았습니다. 다른 두 가지 주요 비용 요소 영역에서도 비슷한 격차가 나타났습니다 (그림 27 참조).

주요 비용 완화 요인의 높은 수준과 낮은 수준 비교
직원 교육 수준이 낮은 조직의 평균 유출 비용은 510만 달러로, 직원 교육 수준이 높은 조직의 평균 유출 비용 415만 달러보다 높았습니다. 다른 두 가지 주요 비용 요소 영역에서도 비슷한 격차가 나타났습니다 (그림 28 참조).

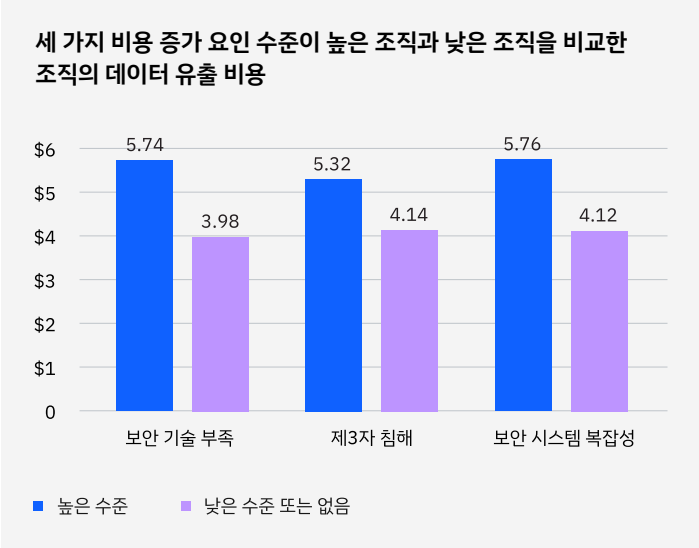


그림 27. 미화 100만 달러로 측정

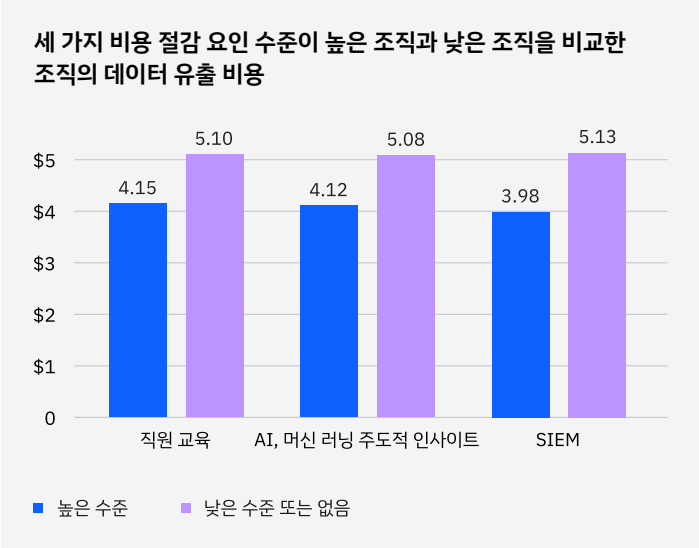


그림 28. 미화 100만 달러 단위 기재

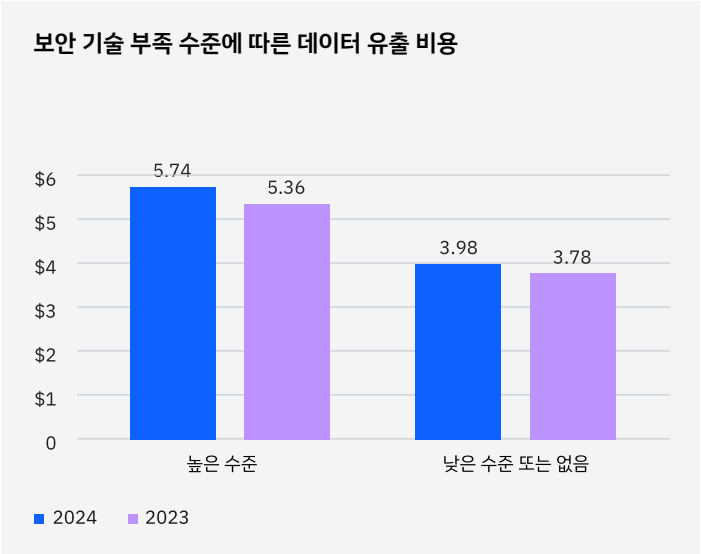


그림 29. 미화 100만 달러로 측정

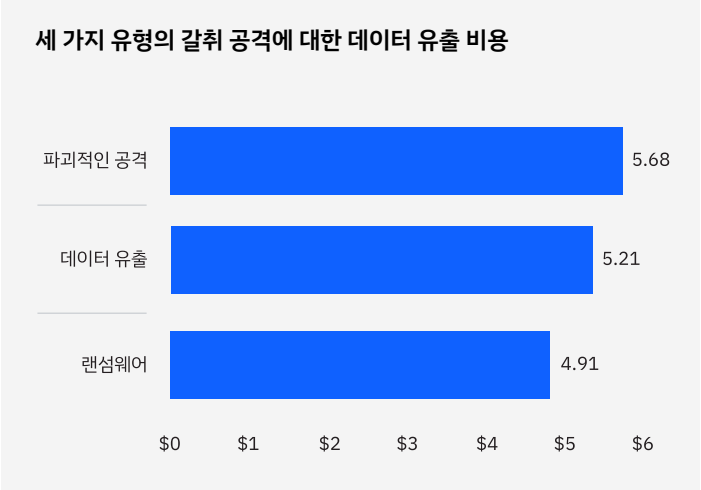


그림 30. 미화 100만 달러 단위로 측정

보안 기술 부족

숙련된 보안 인력이 심각하게 부족한 조직의 수는 2024년 53%로, 작년 42%에 비해 많이 증가했습니다. 올해 연구 결과 악화되는 기술 부족과 데이터 유출 비용 증가 사이에 밀접한 연관성이 있는 것으로 나타났습니다.

기술 부족으로 유출 비용 증가
2024년 고급 기술 부족으로 인한 평균 유출 비용이 작년 536만 달러에서 7.1% 증가한 574만 달러로 급증했습니다. 이는 전 세계 평균 유출 비용보다 86만 달러 높은 수치입니다 (그림 29 참조).

탈취 공격 비용

조직이 탈취 공격으로 인해 지출하는 금액은 랜섬웨어, 데이터 유출(data exfiltration) 및 파괴적 공격과 같은 유형에 따라, 또한 조직의 대응 방식에 따라 달라질 수 있습니다. 이 요소는 특히 사법 기관이 개입하는 경우 더욱 그러한데, 올해 연구에 따르면 사법 기관의 수사가 개입했을 때 비용이 많이 감소한 것으로 나타났습니다. 데이터를 암호화하고 몸값을 요구하는 랜섬웨어, 데이터를 훔치고 조직을 갈취하기도 하는 데이터 유출(data exfiltration), 공격자가 자신의 목적을 위해 데이터를 삭제하고 파괴하는 파괴적 공격 등 세 가지 유형의 공격을 모두 조사했습니다.

다른 탈취보다 더 큰 비용을 발생시키는 파괴적 공격
파괴적 공격, 즉 항구적이고 비용이 많이 드는 손상을 입히기 위한 공격 때문에 드는 평균 비용은 568만 달러에 달했으며 랜섬웨어 공격이나 데이터 유출(data exfiltration) 공격보다 더 큰 비용이 소요되는 것으로 나타났습니다 (그림 30 참조).

63%

사법 기관이 개입한 랜섬웨어 피해자 중 몸값을 지불하지 않은 비율

세 가지 유형의 탈취 공격 파악 및 억제에 드는 시간
세 가지 유형의 공격을 파악하고 억제하는 데 모두 284~294일이 소요되었습니다 (그림 31 참조).

몸값 지불
조직이 랜섬웨어의 피해를 입었을 때 52%가 사법 기관에 신고했습니다. 신고한 조직의 대부분, 즉 63%가 몸값을 지불하지 않았습니다 (그림 32 참조).

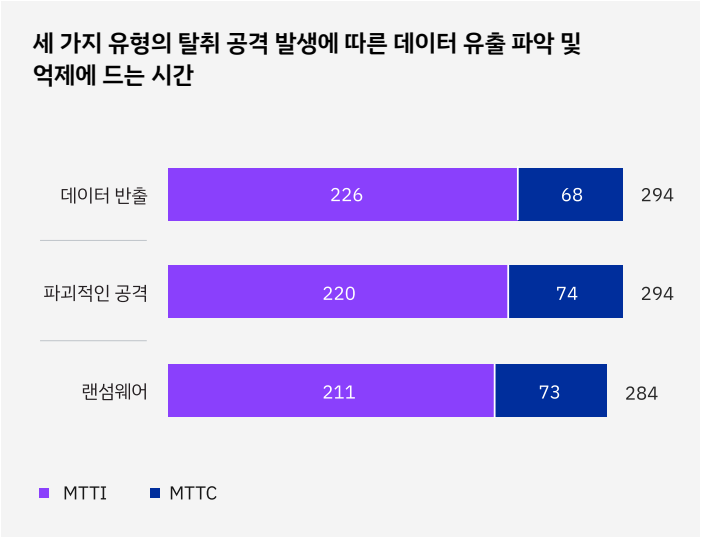


그림 31. 일 단위

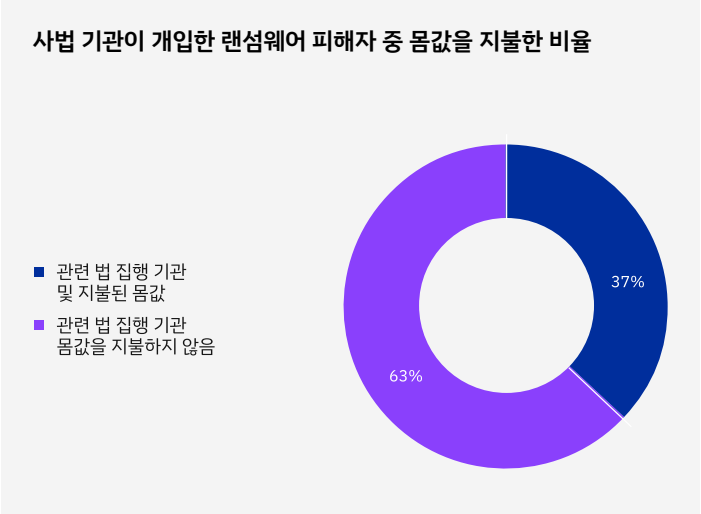


그림 32.

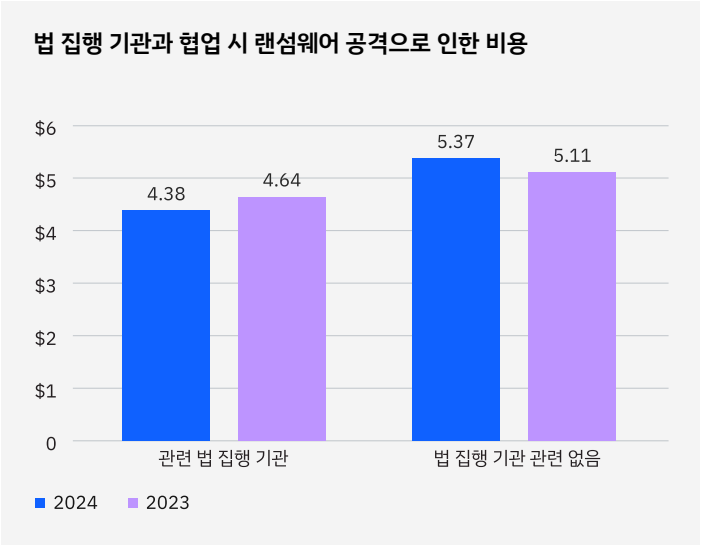


그림 33. 미화 100만 달러로 측정

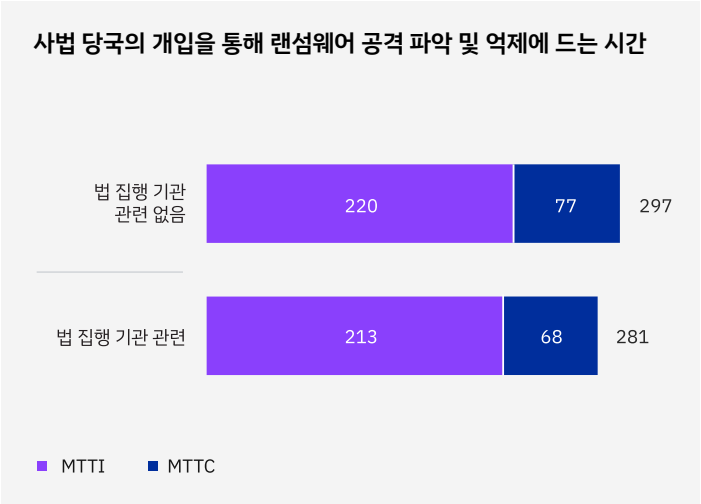


그림 34. 일 단위

사법 기관 개입을 통한 유출 비용 감소

평균 유출 비용은 사법 기관이 개입한 경우 438만 달러, 사법 기관이 개입하지 않은 경우 537만 달러로, 20% 이상, 거의 100만 달러의 비용 차이가 났습니다. 참고로, 이 비용 수치에는 몸값 지불 비용이 포함되지 않았습니다 (그림 33 참조). 또한 사법 기관 개입을 통해 유출을 파악하고 억제하는 데 드는 시간이 단축되었습니다 (그림 34 참조).

↑22.7%

5만 달러 이상의 벌금을 납부하는 조직의 비율 증가

유출 및 규제 벌금 신고

올해 보고서에 따르면 대부분의 조직이 규제 당국이나 기타 정부 기관에 유출 사실을 신고한 것으로 나타났습니다. 약 1/3은 벌금을 납부했습니다. 결과적으로, 신고와 벌금 납부가 유출 후 대응의 일반적인 과정이 되었습니다. 이 연구에서는 벌금 규모와 조직이 규제 당국에 유출 사실을 알리는 데 드는 시간을 조사했습니다. 조직 대부분은 며칠 내에 유출 사실을 보고했습니다.

평균 유출 보고 시간
절반 이상의 조직이 72시간 내에 데이터 유출을 보고했으며, 34%는 보고하는 데 72시간 이상이 걸렸습니다. 보고할 의무가 전혀 없는 경우는 11%에 불과했습니다 (그림 35 참조).

규제 벌금 금액 증가
더 많은 조직이 더 높아진 벌금을 납부했는데, 5만 달러 이상의 벌금을 납부한 조직은 작년에 비해 22.7% 증가했으며 10만 달러 이상의 벌금을 납부한 조직은 19.5% 증가했습니다 (그림 36 참조).

규정상 의무로 인해 유출을 신고해야 했나요? 그렇다면 유출 발견 후 신고하는 데 얼마나 걸렸나요?

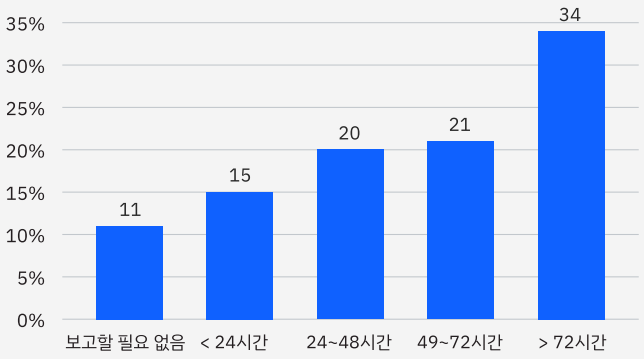


그림 35. 모든 유출 비용, 단수 응답만 허용

데이터 유출로 인해 발생하는 벌금 비용의 분배

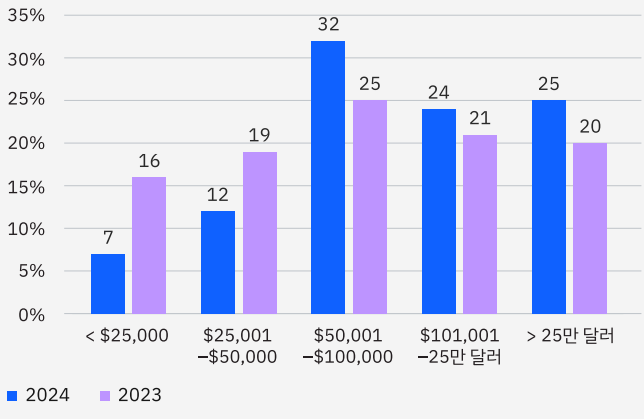


그림 36. 벌금이 부과된 조직 중(미화로 측정)

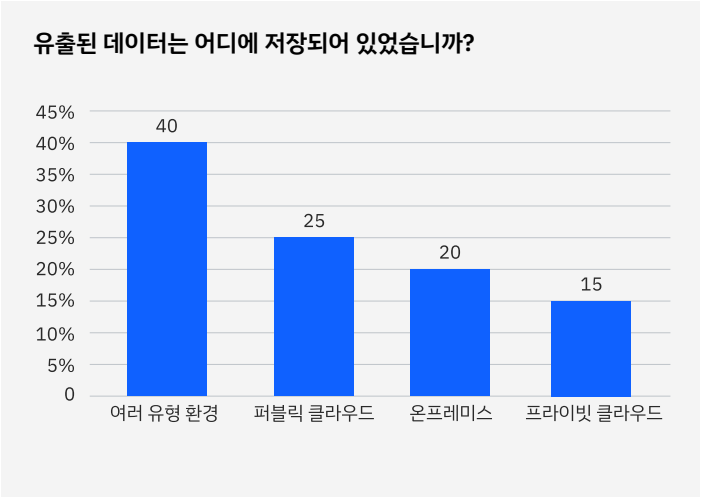


그림 37. 모든 조직 비율. 단수 응답 허용

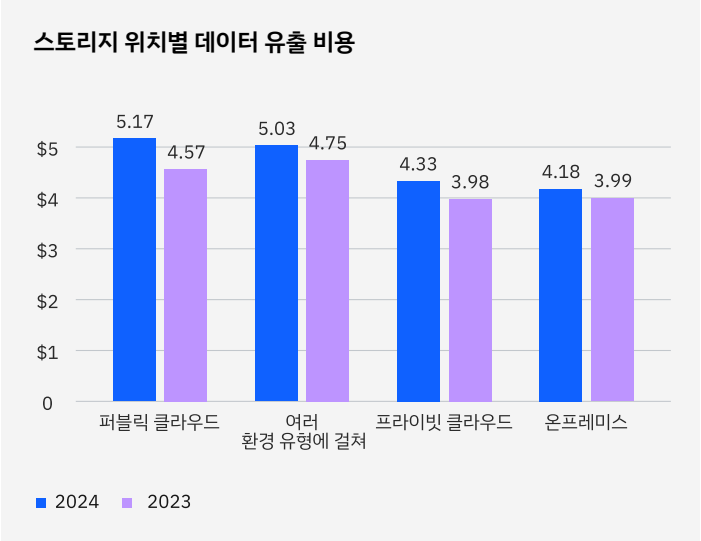


그림 38. 미화 100만 달러로 측정

데이터 보안

데이터가 어디에 저장되어 있든, 데이터는 유출에 취약할 수 있습니다. 올해 연구에 따르면 어떤 위치가 다른 위치보다 더 취약하고 다른 위치보다 유출당 비용이 더 많이 드는 것으로 나타났습니다. 유출 대부분은 여러 환경 또는 퍼블릭 클라우드에 분산된 데이터와 관련이 있습니다. 두 가지 스토리지 옵션 모두 유출 라이프사이클이 길어지고 유출 비용이 커지는 것과 관련이 있었습니다.

조직이 데이터 관리 전략을 확장하고 개선하더라도 관리되지 않고 IT 부서의 눈에 띄지 않는 데이터인 섀도 데이터를 간과하는 경우가 많습니다. 이는 작업자가 승인되지 않은 애플리케이션을 통해 데이터를 공유하거나 비공식 클라우드 버킷에 업로드한 결과일 수 있습니다. 이 보고서에 따르면 섀도 데이터와 관련된 유출은 피해가 더 오래 지속되고 비용이 더 많이 드는 것으로 나타났습니다.

클라우드 유출

데이터 위치별 유출
전체 유출의 약 40%는 퍼블릭 클라우드, 프라이빗 클라우드, 온프레미스와 같은 여러 환경에 분산된 데이터와 관련된 것이었습니다. 이번 연구에서 퍼블릭 클라우드, 프라이빗 클라우드 또는 온프레미스에만 저장된 데이터와 관련된 유출 사례는 거의 없었습니다. 데이터가 여러 환경에서 더 동적이고 활발하게 사용될수록 데이터를 검색, 분류, 추적하고 보안을 유지하기가 더 어려워졌습니다 (그림 37 참조).

위치 및 비용별 유출
퍼블릭 클라우드에서만 발생한 데이터 유출은 평균 517만 달러의 비용을 발생시켰으며, 이는 작년보다 13.1% 증가한 것으로 데이터 유출 유형 중 가장 많은 피해액을 초래했습니다. 여러 환경으로 인한 유출이 더욱 흔하긴 했지만, 퍼블릭 클라우드 유출보다 비용이 더 적게 발생했습니다. 온프레미스 유출이 비용이 가장 적게 발생했습니다 (그림 38 참조).

527만 달러

섀도 데이터 관련 데이터 유출
평균 비용

신속한 문제 해결과 관련된 중앙 집중식 통제
데이터를 중앙 집중식으로 제어할 수 있는 조직일수록 평균적으로 더 빨리 유출을 파악하고 억제할 수 있었습니다. 온프레미스에만 저장된 데이터에 발생한 유출은 파악 및 억제에 평균적으로 224일이 소요되어, 이는 여러 환경에 분산된 데이터의 경우 283일이 소요된 것에 비해 23.3% 더 짧은 시간이 걸렸습니다. 프라이빗 클라우드 아키텍처와 퍼블릭 클라우드 아키텍처의 비교에서도 동일한 패턴의 로컬 제어 및 단축된 유출 라이프사이클이 나타났습니다(그림 39 참조).

섀도 데이터

섀도 데이터에 관한 유출 비용
섀도 데이터가 포함된 데이터 유출의 평균 비용은 527만 달러로 섀도 데이터가 없는 유출의 평균 비용보다 16.2% 더 높았습니다(그림 40 참조).

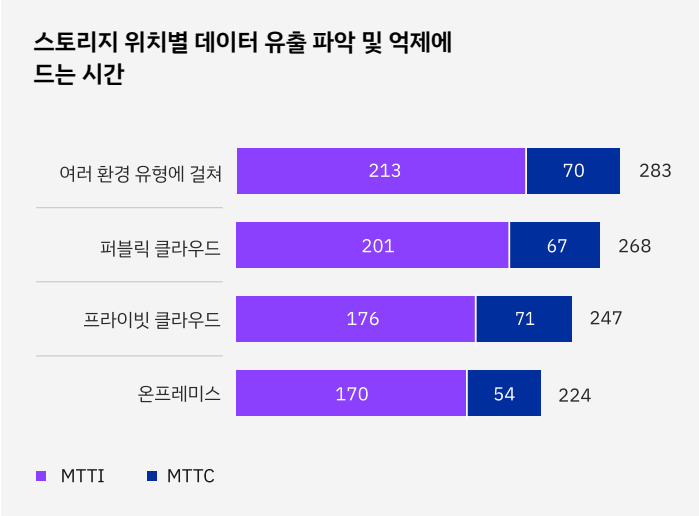


그림 39. 일 단위

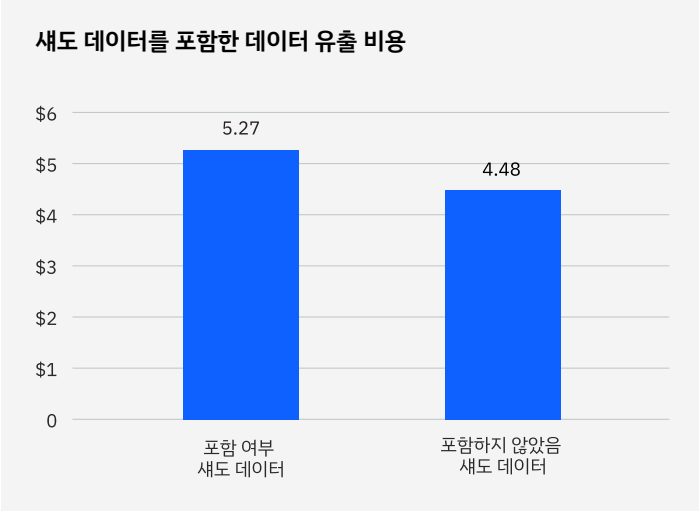


그림 40. 미화 100만 달러로 측정

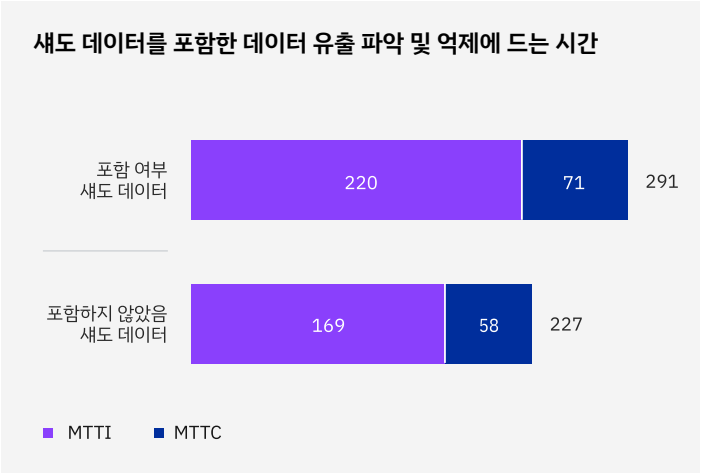


그림 41. 일 단위

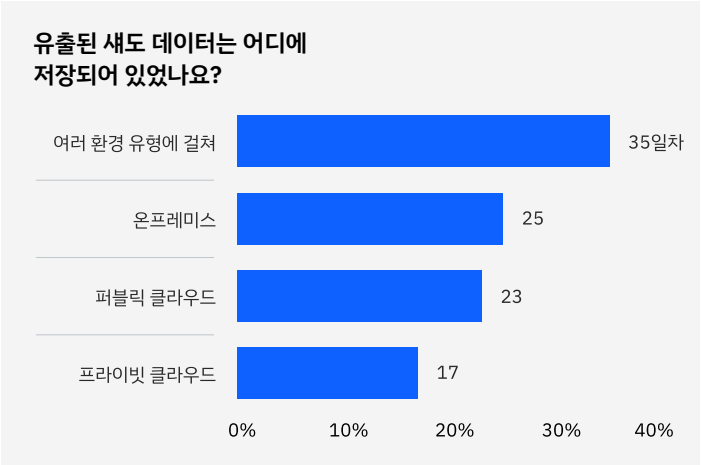


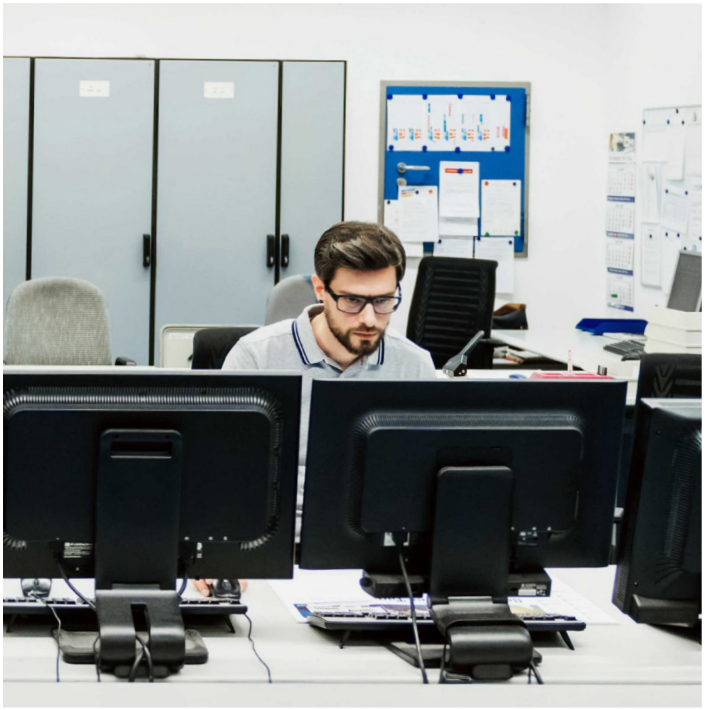
그림 42. 섀도 데이터 관련 유출 비율(단수 응답만 허용)

섀도 데이터의 유출 라이프사이클

섀도 데이터를 포함하는 유출은 그렇지 않은 유출보다 파악하는 데 평균 26.2%, 억제하는 데 평균 20.2% 더 오래 걸렸습니다. 이러한 증가로 인해 데이터 유출의 평균 라이프사이클이 291일로, 섀도 데이터가 없는 데이터 유출보다 24.7% 더 오래 지속되었습니다(그림 41 참조).

여러 환경 전반의 섀도 데이터

섀도 데이터는 퍼블릭 및 프라이빗 클라우드, 온프레미스와 같은 모든 유형의 환경에서 발견되었지만, 섀도 데이터가 포함된 유출의 25%는 온프레미스 환경에서만 발생했습니다. 이러한 발견은 섀도 데이터가 꼭 클라우드 스토리지와 관련된 문제가 아니라는 것을 의미합니다(그림 42 참조).



대규모 유출

100만 건 이상의 기록 유출이 특징적인 대규모 유출은 상대적으로 드문 편입니다. 따라서 이 연구에서는 대량 유출을 대부분의 다른 유출과 별도로 다루어 일반적인 데이터 유출에 대한 분석을 왜곡하지 않도록 했습니다.

대규모 유출 비용 증가
모든 대규모 유출 범주의 평균 비용은 작년보다 올해 더 높았습니다. 이러한 증가는 5,000~6,000만 건의 기록에 영향을 미친 대규모 유출에서 가장 두드러졌습니다. 평균 비용이 13% 증가했으며, 이러한 유출은 일반적인 유출보다 몇 배나 더 많은 비용이 들었습니다. 100만~1,000만 건의 기록에 영향을 미친 가장 미약한 수준의 대규모 유출의 경우에도 평균 비용은 전 세계 평균 비용의 9배에 달하는 488만 달러였습니다(그림 43 참조).

손실 기록별 대규모 유출의 비용

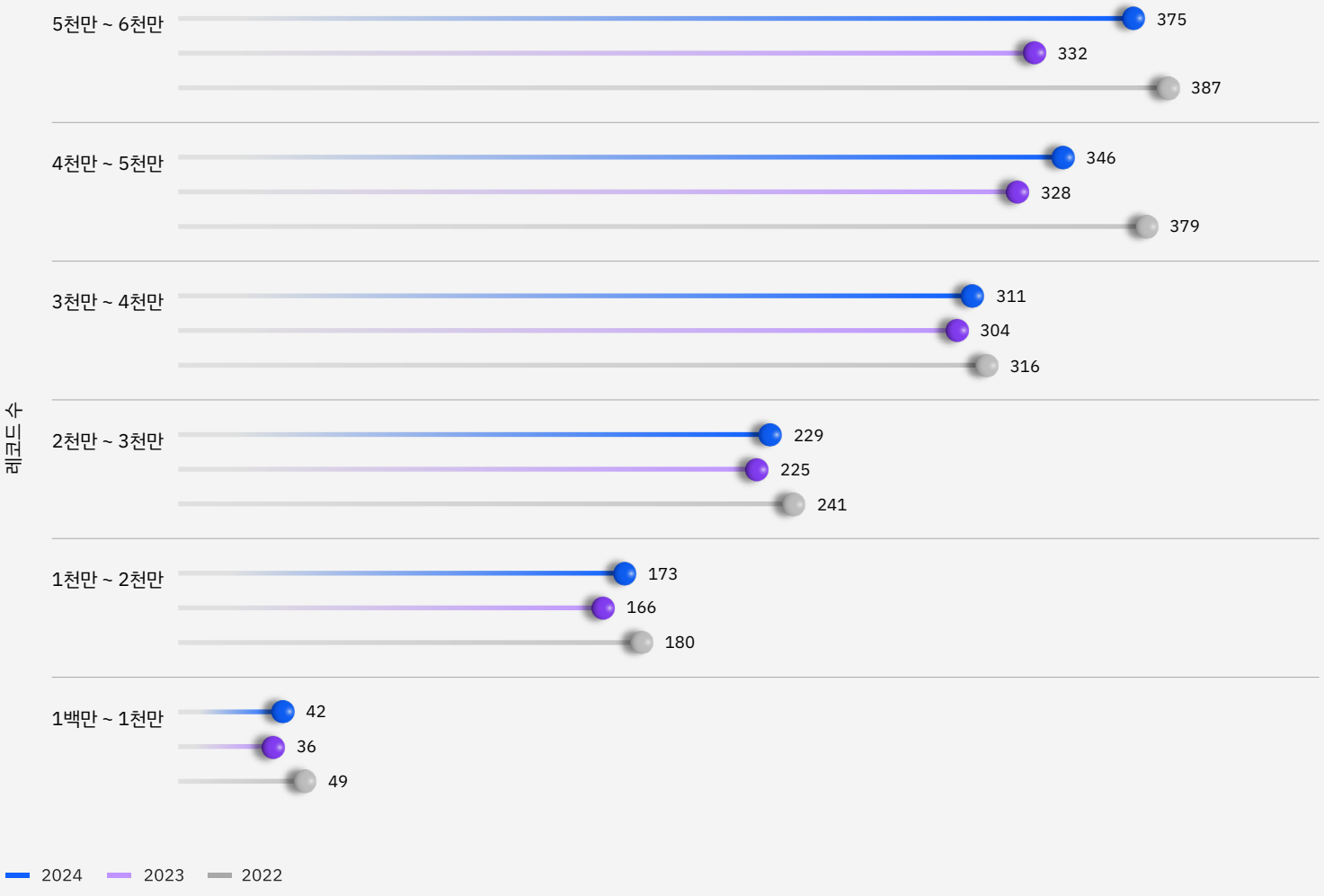


그림 43. 미화 100만 달러로 측정

↑23.5%

유출 이후 보안 투자를 강화할 계획이 있는 조직의 비율 증가

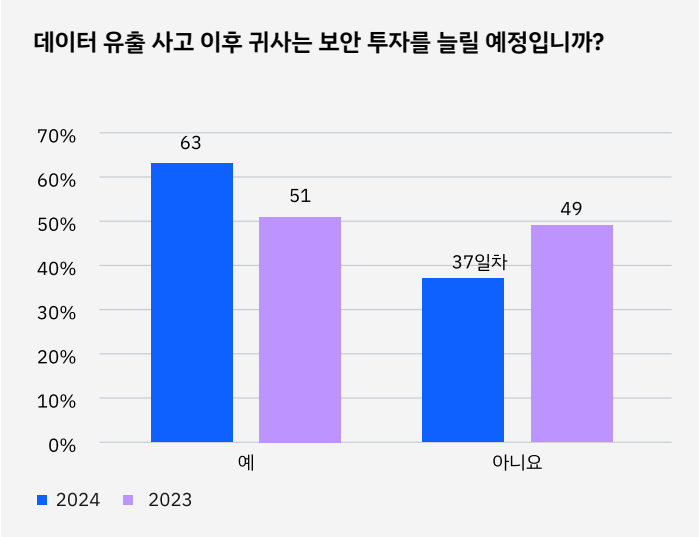


그림 44. 모든 조직 비율

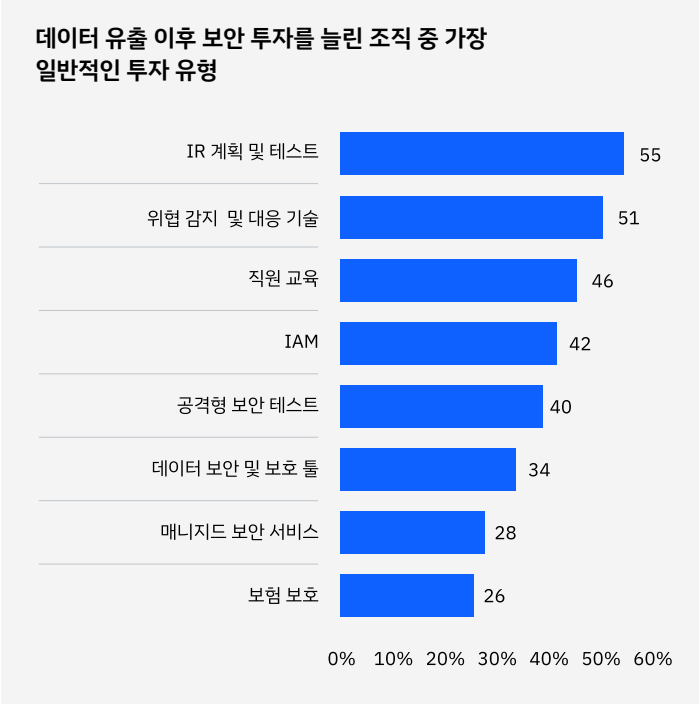


그림 45. 보안 투자를 늘리는 조직 비율(복수 응답 허용)

보안 투자

조직에 유출이 발생하면 비즈니스와 IT 리더는 보안 투자를 늘리는 경우가 많습니다. 올해 연구에서는 조직에게 향후 보안 관련 지출 계획에 대해 물었습니다. 조직은 1개 이상의 투자 영역을 파악할 수 있었습니다.

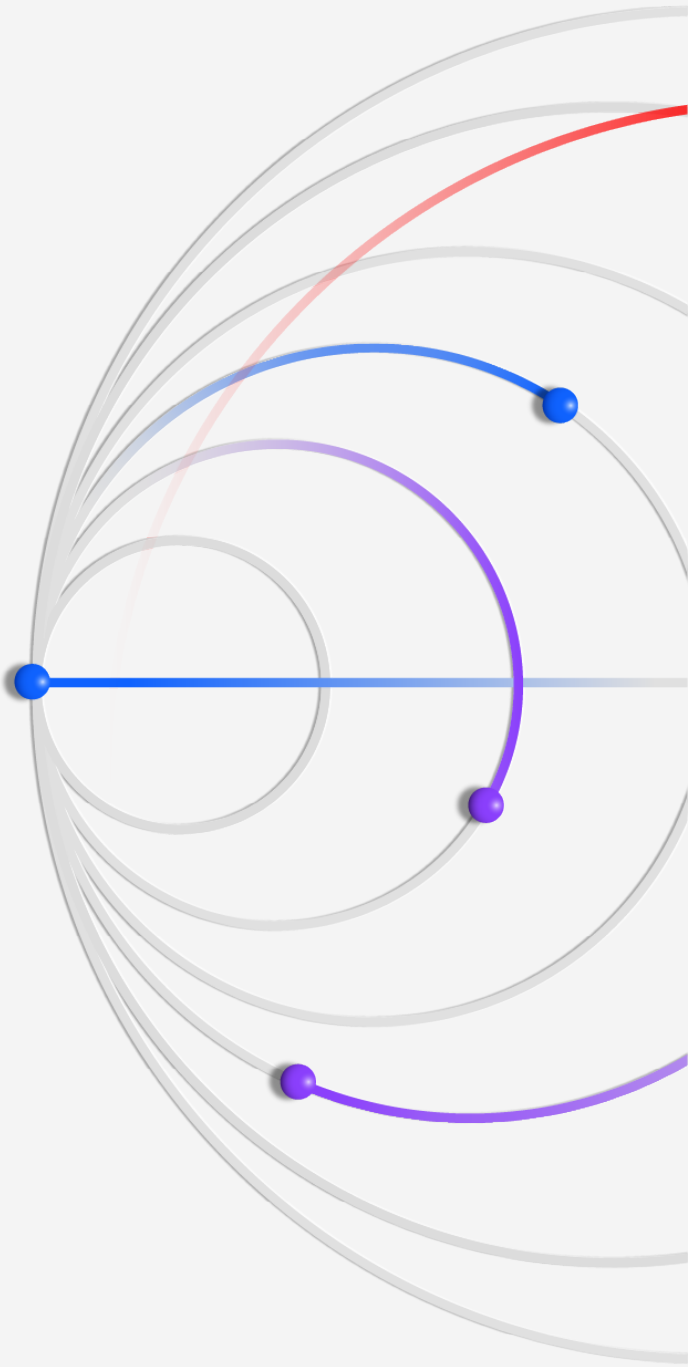
보안 투자를 늘리는 조직 비율의 증가

유출 이후 조직의 거의 3분의 2가 보안 투자를 늘리겠다고 계획했으며, 이는 작년에 비해 23.5% 증가한 수치입니다. 이러한 증가는 비즈니스 손실 및 규제 벌금과 관련된 유출 비용이 평판 손상 가능성과 함께 계속해서 증가하고 있다는 현실을 반영한 것일 수 있습니다(그림 44 참조).

인기 있는 보안 투자 영역

올해 가장 인기 있는 두 가지 보안 투자 영역은 IR 계획 및 테스트(55%)와 위협 탐지 및 대응 기술(51%)이었습니다. 상위 두 가지 투자 영역은 수상한 인시던트와 위협을 탐지하고 더 신속하게 대응하는 데 중점을 두었습니다. 또한 많은 조직이 데이터 보안 및 보호 툴(34%)과 IAM(42%)에 투자할 계획이 있다고 했습니다(그림 45 참조).

데이터 유출 비용을 줄이는 데 도움이 되는 권장 사항



권장 사항에는 비용을 절감하고 유출 식별 및 억제에 소요되는 시간을 단축할 수 있는 성공적인 보안 접근 방식이 포함됩니다.

정보 환경 파악하기

대부분의 조직에서는 온프레미스 데이터 저장소, 프라이빗 클라우드, 퍼블릭 클라우드 등 각종 환경에 데이터를 배포합니다. 그러나 상당수의 조직이 불완전하거나 오래된 데이터 재고를 보유하고 있는 탓에 어떤 데이터가 유출되었는지, 그리고 유출된 데이터의 민감도 또는 기밀 등급이 얼마나 되는지 파악하기 위한 조치가 지연되곤 합니다. 이 같은 지연으로 인해 대응이 복잡해지고 데이터 유출 비용이 증가할 수 있습니다.

보안팀은 데이터의 위치와 관계없이 지속적으로 데이터를 모니터링하고 보호할 수 있도록 앞서 설명한 모든 환경에 대해 종합적인 시야를 유지해야 합니다. 조직에서는 데이터 보안 태세 관리(DSPM) 및 기타 솔루션(예: ID 접근 권한 관리 및 ASM)을 적용함으로써, 이 모든 환경을 통틀어 일관적이고 종합적인 보호 조치를 시행합니다.

보안팀은 하이브리드 환경 및 퍼블릭 클라우드를 각별히 주의해야 합니다. 데이터 유출 사고의 40%는 여러 환경에 저장된 데이터와 관련이 있었죠. 또한 유출된 데이터가 퍼블릭 클라우드에 저장된 경우에는 평균 유출 비용이 517만 달러로, 유출로 인해 발생한 비용 중 가장 높았습니다. 따라서 보안팀은 자신들이 이용하는 각 클라우드 서비스의 특정 위험 및 제어 수단에 대해 보다 세밀하게 이해해야만 합니다.

관리 대상이 아닌 데이터의 영향으로 인해 모든 환경을 아우르는 데이터 관리가 더욱 복잡해졌습니다. 데이터 유출 사고의 1/3 이상은 섀도 데이터와 관련이 있죠. 보안팀은 앞으로 관리 대상이 아닌 데이터 소스가 조직에 존재한다고 가정해야 합니다. AI 워크로드 내부의 데이터와 같이 암호화되지 않은 데이터 때문에 위험이 더욱 커질 수 있으니까요. 데이터 유출 시 위험을 낮추기 위해서는 데이터 암호화 전략을 세울 때 데이터의 종류, 용도 및 존재 위치를 고려해야 합니다.

AI 및 자동화를 통한 예방 전략 강화

조직 전반에 걸쳐 생성형 AI 모델과 서드파티 애플리케이션을 도입하는 한편, 사물인터넷(IoT) 기기와 SaaS 애플리케이션을 지속적으로 사용함에 따라 공격 표면이 확장되면서 보안팀이 압박을 받고 있습니다.

보안 예방 전략(ASM, 레드팀 구성, 태세 관리 등의 영역 포함)에 도움이 되도록 AI 및 자동화를 적용하는 것은 관리형 보안 서비스로 해결되는 경우가 많습니다. 금년도 연구 결과에 따르면, AI 및 자동화를 적용한 조직들은 다른 세 영역인 감지, 조사, 대응 영역에 비해 보안 예방 영역에서 AI 투자 효과를 가장 크게 보았습니다. 이 조직들은 예방 기술에 AI를 적용하지 않은 조직들에 비해 평균 미화 222만 달러를 절약했습니다.

생성형 AI 도입 시 보안을 최우선 순위로 두기

최근 조직들이 생성형 AI 도입을 빠르게 추진하고는 있지만, 생성형 AI 이니셔티브의 24%만이 안전한 상태로 운용되고 있습니다. 보안 수준이 낮으면 데이터와 데이터 모델이 위험에 노출되기 쉬워지고 생성형 AI 프로젝트를 통해 제공될 이익이 훼손될 가능성이 생깁니다.

생성형 AI 도입이 계속해서 확대될수록 조직에 필요한 것은 바로 생성형 AI 데이터 보호, 모델 및 사용량 보호 및 AI 거버넌스 관리 체제 구축을 위한 프레임워크입니다. 이외에도 조직은 도용과 조작으로부터 데이터를 보호해서 학습 데이터를 확보해야 합니다. 조직은 데이터 디스커버리 및 분류를 이용해서 학습 또는 미세 조정에 사용될 민감 데이터를 찾아낼 수 있습니다. 암호화, 접근 권한 관리 및 규정 준수 모니터링 등을 아우르는 데이터 보안 제어 조치를 시행할 수도 있습니다.

조직은 생성형 AI를 사용함에 따라 섀도 데이터의 위험과 그러한 데이터의 증가는 물론, 섀도 모델의 존재까지도 알게 됩니다. 조직은 민감한 AI 학습 데이터를 보호하고, 비승인 또는 섀도 AI 모델 사용과 AI 오용 또는 데이터 유출에 대한 시야를 확보할 수 있도록 태세 관리를 AI 모델 자체로 확대해야 합니다.

생성형 AI 모델 개발을 안전하게 진행하려면 파이프라인 내부의 취약점을 파악하고, 통합을 강화하고, 정책 및 접근 체제를 시행해야 합니다. 생성형 AI 모델을 안전하게 사용하려면 보안팀을 통해 악의적인 입력(예: 프롬프트 인젝션) 및 민감 데이터가 포함된 아웃풋을 모니터링해야 합니다. 이에 더하여 데이터 포이즈닝, 모델 회피, 모델 추출 등의 AI 특정 공격을 감지하고 이에 대응할 수 있는 AI 보안 솔루션을 보급해야 합니다. 접근을 거부한 후 손상된 모델을 격리하고 연결을 끊는 대응 지침을 개발하는 일도 필수입니다.

생성형 AI 및 기타 IT 이니셔티브로 인해 위협적인 환경이 확대되고 있는 요즘에는 AI 팀에서 근무하는 데이터 과학자, 데이터 엔지니어 등등 보안 외 분야 실무자도 보안 교육을 받아야 합니다.

사이버 대응 훈련 강도 높이기

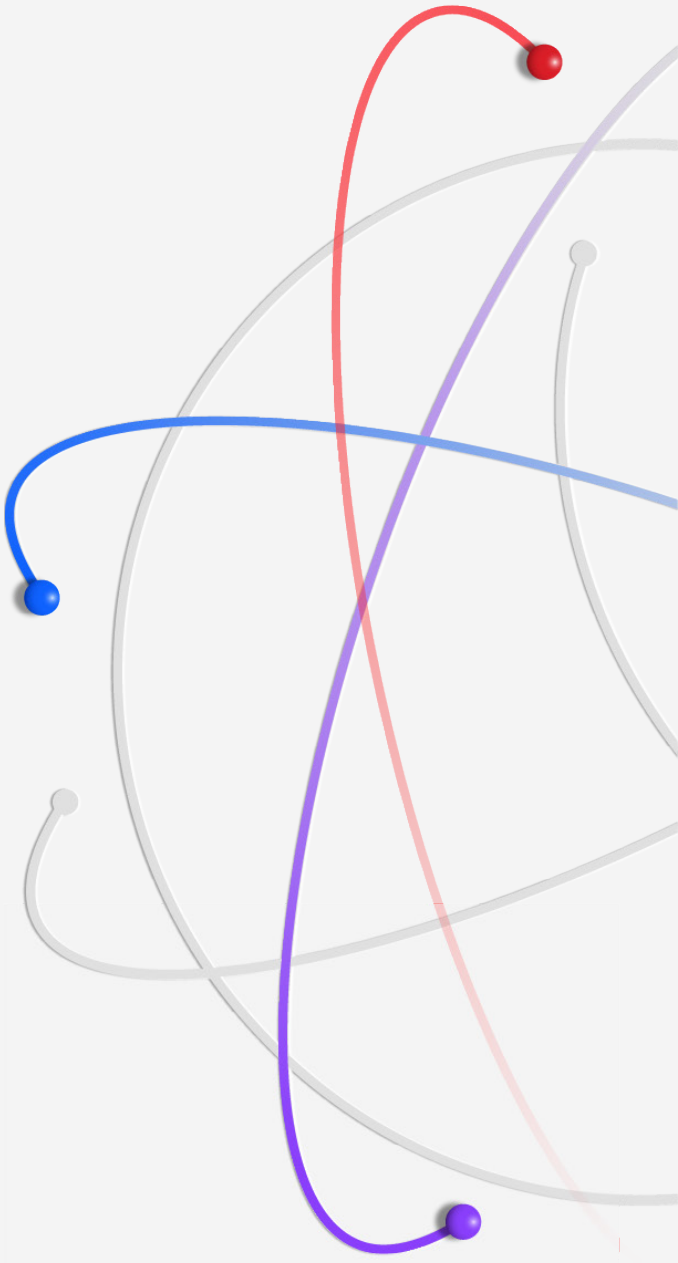
유출 발생 시와 그 이후 조직이 비즈니스 리더십, 규제 기관 및 고객과 어떻게 대응하고 소통하는지가 그 어느 때보다 중요해졌습니다. 막대한 영향을 미치는 공격에 대처하는 능력을 향상하기 위해 조직은 사이버상 위기 시뮬레이션 연습에 참여해 유출 대응 역량을 키울 수 있습니다.

이 훈련에는 보안팀은 물론 경영 책임자도 참여할 수 있으므로, 조직 전체가 데이터 유출을 감지 및 방지하고 이에 대응하는 능력이 향상될 수 있습니다. 보안 책임자는 조직 전반의 경영 실무자 및 커뮤니케이션팀과의 사전 협업을 통해 대응 계획의 초안을 작성하고 시범 실시해야 합니다. 생성형 AI 및 기타 IT 이니셔티브로 인해 위협적인 환경이 확대되고 있는 요즘에는 보안 외 분야 실무자도 보안 교육을 받아야 합니다. 이러한 실무자로는 머신 러닝 팀 및 AI 팀에서 근무하는 데이터 과학자 및 데이터 엔지니어, 온프레미스/클라우드 자산 전반에 걸쳐 AI 워크로드의 지속성을 관리하는 담당자 등이 있습니다.

조직은 대응을 대비하고자 투자함으로써 데이터 유출로 인한 비용과 혼란을 줄이고, 운영 지속성을 높이고, 고객, 파트너 및 기타 주요 이해관계자와의 관계를 유지할 수 있습니다. 또한 대비 상태가 우수한 경영진이 공격의 급성 단계를 처리, 통제 및 전달하기 때문에, 대응 작업을 훈련해 두면 직원들이 안심하면서 조직 내부의 압박감, 고충, 마찰을 덜 수 있습니다.

조직 인구 통계

올해 연구는 16개 국가 및 지역, 17개 산업에서 다양한 규모의 604개 조직을 선정하여 조사했습니다. 이 섹션은 연구 대상 조직을 지역 및 산업별로 살펴보고 산업 분류를 정의합니다.



지역 인구 통계

2024년 연구는 16개 국가와 지역에서 수행되었습니다. 올해 연구에 새롭게 추가된 지역은 베네룩스 지역으로, 벨기에와 네덜란드, 룩셈부르크의 경제 연합입니다. 스칸디나비아 지역은 연구 대상에서 제외되었습니다.

ASEAN은 싱가포르, 인도네시아, 필리핀, 말레이시아, 태국, 베트남에 위치한 조직의 클러스터 샘플입니다. 라틴 아메리카는 멕시코, 아르헨티나, 칠레 및 콜롬비아에 위치한 조직의 클러스터 샘플입니다. 중동은 사우디아라비아와 아랍에미리트에 위치한 조직의 클러스터 샘플입니다.

글로벌 연구 한 눈에 보기

국가 및 지역	2024년 샘플	전체 샘플의 비율	연구 기간	통화
아세안	25	4%	8	싱가포르 달러(SGD)
오스트레일리아	27	4%	15	호주 달러(AUD)
베네룩스	32	5%	1	유로(EUR)
브라질	45	7%	12	브라질 헤알(BRL)
캐나다	28	5%	10	캐나다 달러(CAD)
프랑스	36	6%	15	유로(EUR)
독일	47	8%	16	유로(EUR)
인도	53	9%	13	인도 루피(INR)
이탈리아	29	5%	13	유로(EUR)
일본	42	7%	13	엔(JPY)
라틴 아메리카	28	5%	5	멕시코 페소(MXN)
중동	39	6%	11	사우디아라비아 리얄(SAR)
남아프리카 공화국	24	4%	9	남아프리카공화국 랜드(ZAR)
한국	28	5%	7	원(KRW)
영국	50	8%	17	파운드(GBP)
미국	71	12%	19	미국 달러(USD)
합계	604	100%		

그림 46. 연구에 참여한 모든 조직의 비율

산업 인구 통계

17개의 산업이 이 연구에 선택되었으며, 이 선정은 수년 간의 연구에 걸쳐 변함없이 유지되었습니다. 올해는 금융, 공업, 전문 서비스, 기술과 같은 상위 네 개의 조직이 604개의 연구 대상 중 47%를 차지했습니다.

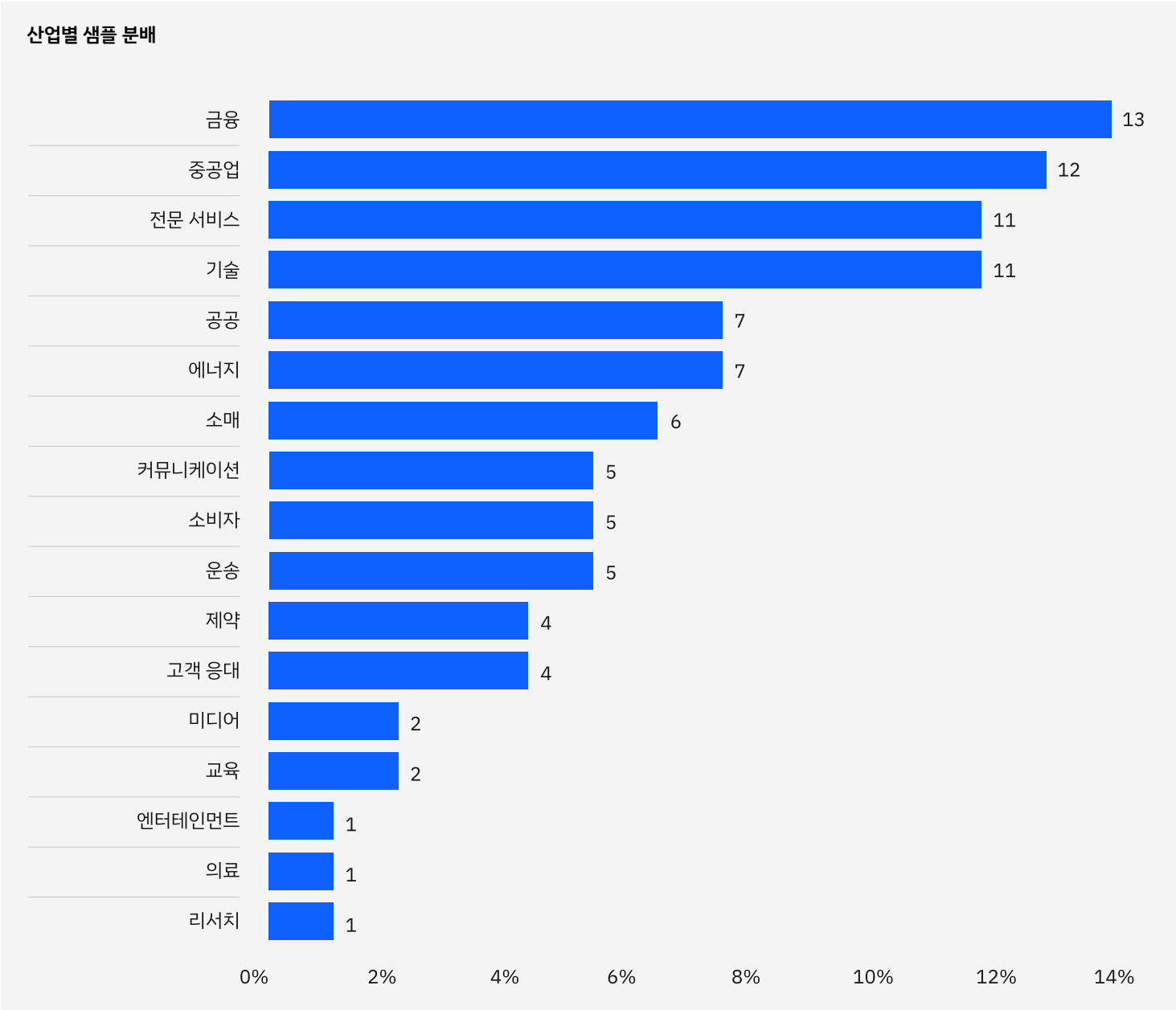


그림 47. 연구에 참여한 모든 조직의 비율

산업 정의

의료
병원, 진료소

금융
은행, 보험, 투자 회사

에너지
정유·가스 회사, 공공 서비스, 대체 에너지 생산업체와 공급업체

제약
생물의학/생명과학 등 제약 회사

중공업
화학 처리, 엔지니어링, 제조 회사

기술
소프트웨어 및 하드웨어 회사

교육
공립/사립 대학교, 교육 개발 업체

전문 서비스
법률, 회계, 컨설팅 회사 등 전문 서비스

엔터테인먼트
영화 제작, 스포츠, 게임, 카지노

운송
항공, 철도, 화물 트럭, 배송 업체

커뮤니케이션
신문, 도서 출판사, 홍보, 광고 대행사

소비자
소비재 제조 및 유통 업체

미디어
텔레비전, 위성, 소셜 미디어, 인터넷

고객 응대
호텔, 레스토랑 체인, 크루즈 라인

소매
오프라인·이커머스

리서치
시장 조사, 싱크탱크, 연구 개발

공공
연방/주/시 정부 기관 및 비정부 기구

연구 방법론

기밀 유지를 위해 벤치마크 장비는 회사 관련 정보를 수집하지 못합니다. 데이터 수집 방법에서는 실제 회계 정보를 제외했으며, 대신 참가자들이 수직선에 범위 변수를 표시하여 직접 비용을 예측하는 방법을 사용했습니다. 참가자들에게 각 비용 범주에 대한 하한선과 상한선 사이 한 자리에 수직선을 표시하라고 요청했습니다.

제시된 각 비용 범주에 대한 포인트 추정치 대신 수직선에서 얻은 숫자 값은 기밀 유지는 물론 더 높은 응답률을 보장합니다. 또한 벤치마크 측정에서는 응답자가 간접 비용과 기회 비용에 대한 별도의 두 번째 추정치를 제공해야 합니다.

벤치마킹을 위한 관리 가능한 데이터 세트를 유지하기 위해 이 보고서에는 데이터 유출 비용에 중대한 영향을 미치는 핵심 비용 활동만 포함했습니다. 전문가와의 상의를 바탕으로 고정된 비용 활동 세트를 선정했습니다. 벤치마크 정보를 수집한 후 일관성과 완전성을 유지하기 위해 각 수단을 신중하게 재검토했습니다.

데이터 유출 비용 요인 범위는 개인 정보를 포함하며 광범위한 비즈니스 운영에 적용되는 알려진 범주로 제한되었습니다. 프로세스에 초점을 맞춘 연구를 통해 향상된 품질의 결과를 얻을 수 있을 것이라고 확신했기 때문에 데이터 보호나 개인정보 보호 규정 준수 활동 대신 비즈니스 프로세스에 집중하기로 했습니다.

데이터 유출 비용을 계산하는 방법

데이터 유출의 평균 비용을 계산하기 위해 본 연구는 아주 작은 규모의 유출 및 아주 큰 규모의 유출은 제외했습니다. 2024년 보고서에서 조사한 데이터 유출은 2,100~113,000건의 손상된 기록으로 범위를 한정했습니다. 대규모 유출 비용의 경우 별도의 분석을 통해 조사했으며, 이 방법론은 이 보고서의 '데이터 유출 FAQ' 섹션에서 자세히 설명합니다.

본 연구는 활동을 식별하고 실제 사용에 따라 비용을 할당하는 활동 기반 비용 산출을 사용했습니다. 네 가지의 프로세스 관련 활동, 즉 감지 및 상급자 보고, 알림, 사후 유출 대응 및 비즈니스 손실로 인해 조직의 데이터 유출과 관련된 다양한 지출이 발생합니다.

감지 및 상급자 보고
조직이 유출을 감지할 수 있는 활동은 다음과 같습니다.

- 포렌식 및 조사 활동
- 평가 및 감사 서비스
- 위기 관리
- 경영진 및 이사회와의 의사소통

알림
조직이 데이터 주체, 데이터 보호 규제 기관 및 기타 제3자에 알릴 수 있도록 하는 활동은 다음과 같습니다.

- 이메일, 서신, 아웃바운드 호출 또는 데이터 대상에 대한 일반적인 통지
- 규제 요구사항 결정
- 규제 기관과의 의사소통
- 외부 전문가 참여

사후 유출 응답
유출 피해자가 조직과 상의하고 피해자 및 규제 기관을 위해 구제 활동을 수행할 수 있도록 하는 활동은 다음과 같습니다.

- 헬프데스크, 인바운드 통신
- 신용 모니터링, ID 보호 서비스
- 새 계정 또는 신용카드 발급
- 법적 지출
- 제품 할인
- 규제 벌금

비즈니스 손실
고객 손실, 비즈니스 운영 중단, 수익 손실을 최소화하기 위한 활동은 다음과 같습니다.

- 비즈니스 운영 중단 및 시스템 가동 중단 시간으로 인한 수익 손실
- 고객 손실 및 신규 고객 확보 비용
- 평판 손상 및 영업권 축소

데이터 유출 FAQ

데이터 유출이란 무엇인가요?
데이터 유출은 개인 식별 정보, 금융 계좌 및 의료 계정 세부 정보, 기타 비밀, 기밀 또는 독점 데이터가 포함된 기록이 위험에 노출될 수 있는 상황으로 정의됩니다.
이러한 기록은 파일 형식 또는 종이 형식일 수 있습니다. 본 연구는 2,100 ~ 113,000개의 침해된 기록으로 범위를 한정했습니다.

탈취된 기록이란 무엇인가요?
기록은 기밀이거나 독점적인 기업, 정부, 금융 데이터를 공개하거나 데이터 유출에서 정보가 분실되거나 도난당한 개인을 식별하는 정보입니다. 예를 들어 개인의 이름, 신용카드 정보 및 기타 PII가 있는 데이터베이스나 보험 계약자 이름 및 지불 정보가 담긴 건강 기록이 포함됩니다.

데이터를 어떻게 수집하나요?
연구진은 2023년 3월부터 2024년 2월 사이에 데이터 유출 피해를 입은 604개 조직의 개인을 대상으로 3,556건 이상의 개별 인터뷰를 통해 심층적인 정성적 데이터를 수집했습니다. 인터뷰 대상자는 조직의 데이터 유출과 유출 해결을 위한 비용에 관해 잘 아는 사람들이었습니다. 인터뷰 대상에는 CEO 또는 임원, 운영 책임자, 관리자 또는 재무 책임자, IT 실무자, 사업부 책임자 및 총괄 관리자, 위험 관리 및 사이버 보안 실무자 등이 포함되었습니다. 개인정보 보호를 위해 조직의 특정 정보는 수집하지 않았습니다.

데이터 유출 비용 포함 사항
연구진은 조직에서 발생한 직접 및 간접 비용을 모두 수집했습니다. 직접 비용에는 포렌식 전문가 참여, 아웃소싱 핫라인 지원, 무료 신용 모니터링 가입, 향후 제품·서비스에 대한 할인 등이 포함됩니다. 간접 비용에는 내부 조사 및 커뮤니케이션과 함께 턴오버 또는 고객 획득률 감소로 인한 고객 손실의 추정 가치가 포함됩니다.

본 연구는 데이터 유출 경험과 직접적으로 관련된 이벤트만을 대상으로 했습니다. 유럽연합 일반 개인정보 보호법(General Data Protection Regulation, GDPR), 캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act, CCPA)과 같은 규정은 조직이 사이버 보안 거버넌스 기술에 대한 투자를 늘리도록 권장할 수 있습니다. 하지만 이러한 활동은 본 연구의 데이터 유출 비용에 직접적인 영향을 미치지 않습니다. 전년도와의 일관성을 위해 회계 비용을 조정하는 대신 동일한 통화 변환 방법을 사용했습니다.

벤치마크 연구는 설문조사 연구와 어떻게 다른가요?
데이터 유출 비용 보고서의 분석 단위는 조직이었습니다. 설문 조사 연구의 분석 단위는 개인입니다. 이 연구에는 604개 조직이 참여했습니다.

기록당 평균 비용을 사용하여 수백만 건의 기록 손실 또는 탈취와 관련된 유출 비용을 계산할 수 있나요?
이 연구에서는 기본적으로 기록당 전체 비용을 사용하여 총 수백만 건의 기록에 달하는 하나 또는 여러 개의 유출 비용을 계산하는 것을 고려하지 않습니다. 기록당 비용은 각 이벤트에서 최대 113,000개의 기록이 침해된 수백 건의 데이터 유출 이벤트 연구에서 도출되었습니다. 이 연구는 100만 개 이상의 기록이 관련된 대규모 유출의 영향을 측정하기 위해 해당 규모의 이벤트 표본 17개를 기반으로 하는 시뮬레이션 프레임워크를 사용합니다.

시뮬레이션 방법을 사용하여 대규모 데이터 유출 비용을 예측하는 이유는 무엇입니까?
대규모 유출을 경험한 17개 조직의 표본 규모는 연구의 활동 기반 비용 방법을 사용하여 통계적으로 의미 있는 분석을 지원할 만큼 충분히 크지 않았습니다. 이 문제를 해결하기 위해 반복적인 시도를 통해 가능한 결과, 즉 임의의 결과 범위를 예측할 수 있도록 몬테 카를로(Monte Carlo) 시뮬레이션을 구축했습니다. 총 269,000회 이상의 시도가 이루어졌습니다. 모든 표본 평균에 대한 총 평균은 100만~5,300만 개의 침해된 기록 범위에서 각 데이터 유출 규모 중 가장 가능성이 높은 결과를 제공했습니다.

매년 동일한 조직을 추적하나요?
매년 연구에는 다양한 조직 표본이 사용됩니다. 이전 보고서와의 일관성을 위해 매년 조직의 업종, 직원 수, 지리적 위치, 데이터 유출 규모와 같은 유사한 특성을 가진 조직을 모집해 배정했습니다. 이 연구를 시작한 2005년 이래 6,184개 조직의 데이터 유출 경험을 연구해 왔습니다.

연구 제한사항

본 연구는 이전 연구에서 성공적으로 구축된 기밀 독점 벤치마크 방법을 사용했습니다. 그러나 연구 결과에서 결론을 도출하기 전에 이 벤치마크 연구에 내재된 한계를 신중하게 고려해야 합니다.

비통계적 결과
연구는 대표적인 비통계적 글로벌 기업의 표본을 기반으로 진행했습니다. 표본 추출 방법이 과학적이지 않으므로 통계적 추론, 오차, 신뢰구간은 이러한 데이터에 적용할 수 없습니다.

무응답
무응답 편향은 테스트되지 않았으므로 연구에 참여하지 않은 조직은 기본 데이터 유출 비용 측면에서 상당한 차이가 있을 수 있습니다.

표본 추출틀 편향
표본 추출 프레임에는 주관적인 판단이 개입되어, 프레임이 연구 대상 조직 모집단을 대표하는 정도에 따라 결과가 달라졌습니다. 현재 표본 추출 프레임은 개인정보 보호 및 정보 보안 프로그램이 완성 단계에 있는 조직으로 편향되어있습니다.

조직별 정보
벤치마크는 조직 식별 정보를 담지 않습니다. 개인은 범주 응답 변수를 사용하여 조직 및 산업 범주에 대한 인구 통계 정보를 공개할 수 있습니다.

측정되지 않은 요소
분석에서 주요 경향 및 조직 특성과 같은 변수는 생략되었습니다. 생략된 변수가 벤치마크 결과를 설명할 수 있는지는 판단할 수 없습니다.

추정된 비용 결과
특정 검사와 균형을 벤치마크 프로세스에 통합할 수 있지만, 응답자가 정확하고 신뢰할 수 있는 답변을 제공하지 않을 가능성은 항상 존재합니다. 또한, 실제 비용 데이터 대신 비용 추정 방법을 사용하면 의도치 않게 편향과 부정확성이 발생할 수 있습니다.

통화 변환
현지 통화를 미국 달러로 환산하면 다른 국가의 평균 총 비용 예상치가 축소됩니다. 전년도와의 일관성을 위해 비용을 조정하는 대신 동일한 회계 방법을 계속 사용하기로 결정했습니다. 모든 국가 수준의 결과가 현지 통화로 표시되기 때문에, 이 문제는 글로벌 분석에만 영향을 미칠 수 있다는 점에 유의해야 합니다. 이 연구 보고서에 사용된 시점의 실질 환율은 2024년 3월 4일 연방준비은행에서 발표한 환율입니다.

IBM 및 Ponemon Institute 소개

IBM

IBM은 선도적인 글로벌 하이브리드 클라우드/AI/비즈니스 서비스 제공업체로서 175개국이 넘는 국가의 고객이 데이터에서 얻은 인사이트를 활용하고, 비즈니스 절차를 간소화하고, 비용을 절감하고, 각자의 업종에서 경쟁 우위를 확보할 수 있도록 지원합니다. 이 모든 성과의 원천은 바로 신뢰, 투명성, 책임감, 포용성 및 서비스를 달성하기 위한 IBM의 유서 깊은 헌신입니다.
자세한 내용은 www.ibm.com/kr-ko에서 확인하세요.

보안 태세 강화 자세히 보기:

ibm.com/kr-ko/security를

방문하고 IBM Security 커뮤니티에서 대화에 참여해 보세요.

Ponemon Institute

2002년에 설립된 Ponemon Institute는 기업 및 정부 부처 내부의 책임 있는 정보 및 개인정보 관리 제도를 발전시키기 위한 독립 연구/교육에 전념하고 있습니다. 본 기관의 사명은 사람과 조직에 대한 민감 정보의 관리 및 보안에 영향을 미치는 핵심 문제를 대상으로 수준 높은 실증적 연구를 수행하는 것입니다.

Ponemon Institute는 엄격한 데이터 기밀성, 개인정보 보호 및 윤리적 연구 기준을 준수하며, 기업 연구 과정에서 개인의 개인 식별 정보(PII) 또는 회사 식별 정보를 수집하지 않습니다. 또한 엄격한 품질 기준에 따라 연구 대상자에게 연구와 관계없거나 부적절한 질문을 하지 않습니다.

본 연구 보고서에 대해 질문이나 의견(보고서 인용 또는 재작성에 관한 허가 요청 포함)이 있는 경우 하기 우편, 전화 또는 이메일로 문의하세요.

Ponemon Institute LLC
Research Department
1-800-887-3118
research@ponemon.org

(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)
IBM Corporation
New Orchard Road
Armonk, NY 10504

미국에서
제작
2024년 7월