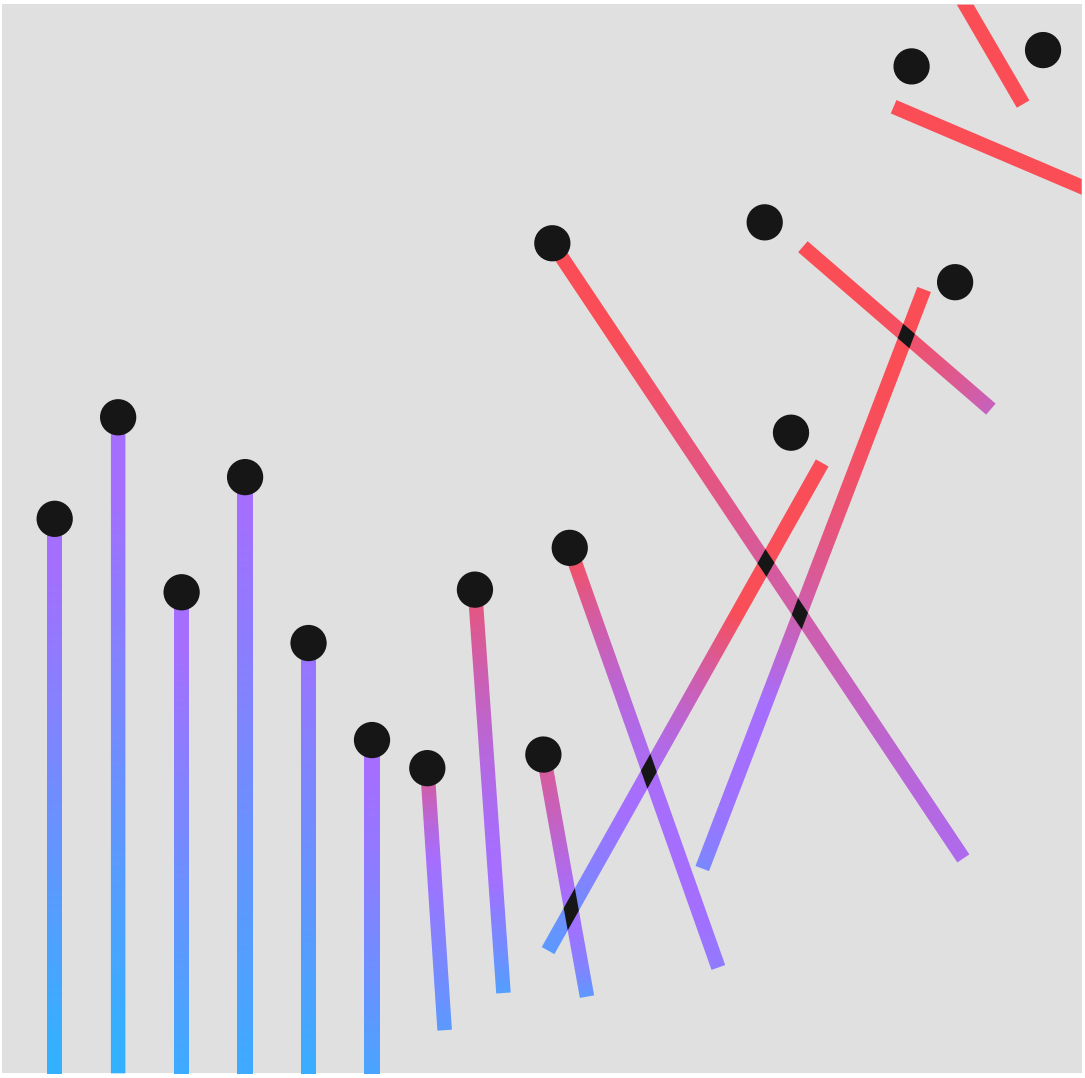
IBM **Security**

2022년 데이터 유출 비용 보고서 핵심 요약



IBM

목차

핵심 요약

본 데이터 유출 비용 보고서는 IT, 위험 관리, 보안 선두기업에 데이터 유출로 인한 비용을 증가시키거나 완화하는 요인을 제시합니다.

올해로 17년 째를 맞이한 본 연구는 Ponemon Institute가 독자적으로 수행하였으며, IBM Security®는 이를 후원하고, 분석하고, 출간하였습니다. 2021년 3월부터 2022년 3월까지 발생한 데이터 유출의 영향을 받은 550개 조직을 대상으로 연구를 실시하였습니다. 해당 기간 17개 국가와 지역, 그리고 17개 업계에서 데이터 유출이 발생하였습니다.

본 연구에서는 데이터 유출의 영향을 받은 조직에 소속된 개인을 대상으로 3,600건 이상의 인터뷰를 수행하였습니다. 인터뷰를 진행하는 동안, 데이터 유출에 대한 즉각적이고 장기적인 대응에 직결된 다양한 조치에 있어서 조직에 소요되는 비용을 파악하기 위해 다수의 질문을 하였습니다.

전년도 보고서와 마찬가지로, 올해 데이터 또한 어떻게 수십 가지 요인이 데이터 유출 발생 이후 계속 증가하는 비용에 영향을 미치는지 보여줍니다. 더불어, 데이터 유출의 근본 원인과 장·단기적 결과, 기업이 손실을 제한할 수 있었던 완화 요인 및 기술에 대해서도 살펴봅니다.

주요 연구 결과

본 보고서에 기술된 주요 결과는 Ponemon Institute에서 수집한 연구 데이터에 대한 IBM Security의 분석에 기반합니다.[1]

미화 435만 달러

데이터 유출로 인한 평균 총비용

데이터 유출로 인한 비용은 2022년 평균 미화 435만 달러로 역대 최고치를 기록했습니다. 이는 평균 유출 비용이 미화 424만 달러였던 지난해보다 2.6% 증가한 수치입니다. 또한 평균 비용은 2020년 보고서에서 밝힌 386만 달러보다 12.7% 증가했습니다.

83%

데이터 유출을 2회 이상 겪은 조직의 비율

조사 대상 조직의 83%는 데이터 유출을 두 번 이상 겪었으며, 17%만이 첫번째 유출 사고라고 응답했습니다. 조사 대상 조직의 60%는 데이터 유출로 인해 서비스 또는 제품의 가격을 인상했다고 응답했습니다.

미화 482만 달러

중요 인프라 데이터 유출로 인한 평균 비용

조사 대상 중요 인프라 조직의 평균 데이터 유출 비용은 미화 482만 달러로, 타 업계의 평균 비용보다 100만 달러나 더 높은 액수입니다. 중요 인프라 조직은 금융 서비스, 공업, 기술, 에너지, 교통, 통신, 의료, 교육, 공공 부문 산업을 포함합니다. 데이터 유출을 겪은 조직 중 28%는 파괴적인 공격이나 랜섬웨어 공격을 당했고, 17%는 보안이 손상된 비즈니스 파트너사로 인해 데이터 유출을 겪었습니다.

미화 305만 달러

보안 AI 및 자동화 완전 배포를 통한 평균 비용 절감

보안 AI와 자동화를 완전히 배포한 조직은 그렇지 않은 조직에 비해 305만 달러나 더 적은 데이터 유출 비용을 지출했습니다. 보안 AI와 자동화를 완전히 배포한 조직의 평균 데이터 유출 비용은 315만 달러, 그렇지 않은 조직은 620만 달러로 무려 65.2%에 달하는 차이를 보였습니다. 이는 본 연구에서 드러난 가장 큰 비용 절감 요소입니다. 또한 유출 행위를 파악하고 억제하는 데 소요되는 시간인 이른바 유출 수명 주기의 경우, 보안 AI와 자동화를 완전히 배포한 기업은 그렇지 않은 기업에 비해 평균 74일이나 더 짧은 수명 주기를 경험하였습니다(완전 배포 시 249일, 미배포 시 323일). 아울러 보안 AI와 자동화 이용률은 2020년 59%에서 2022년 70%로 2년 사이 5분의 1 가까이 급증했습니다.

1. 본 보고서 내 비용 금액은 미국 달러(USD)로 측정합니다.

미화 454만 달러

랜섬웨어 공격으로 인한 평균 비용(랜섬웨어 비용 비포함)

본 연구에서 밝혀진 데이터 유출의 11%는 랜섬웨어 공격에서 비롯되었으며, 이는 데이터 유출 원인의 7.8%가 랜섬웨어였던 2021년에 비해 41%나 증가한 수치입니다. 랜섬웨어 공격으로 인한 평균 비용은 2021년 미화 462만 달러에서 2022년 미화 454만 달러로 소폭 감소했습니다. 이 비용은 데이터 유출로 인한 전체 평균 총비용인 435만 달러보다는 약간 높은 수준입니다.

19%

도난되거나 손상된 권한 정보로 인한 데이터 유출 빈도

도난되거나 손상된 권한 정보를 사용하는 것은 데이터 유출의 가장 일반적인 원인입니다. 2022년 연구에서 도난되거나 손상된 권한 정보는 19%에 달하는 데이터 유출의 주요 공격 벡터였으며, 2021년 연구에서도 최상위 공격 벡터로 20%의 데이터 유출을 유발했습니다. 도난되거나 손상된 권한 정보로 인한 데이터 유출은 평균 미화 450만 달러의 비용을 초래합니다. 또한 가장 긴 수명 주기로 인해 유출을 파악하는 데에만 243일, 유출을 억제하는 데에는 84일이 걸렸습니다. 피싱은 데이터 유출 원인 중 두 번째로 많은 16%를 차지하며, 평균 미화 491만 달러의 가장 비싼 유출 비용을 야기했습니다.

59%

제로 트러스트를 배포하지 않은 조직의 비율

조사 대상 조직 중 41%만이 제로 트러스트 보안 아키텍처를 배포했다고 답했습니다. 제로 트러스트를 배포하지 않은 나머지 59%의 조직은 배포한 조직에 비해 평균 미화 100만 달러 더 많은 유출 비용이 소요됩니다. 79%의 중요 인프라 조직은 훨씬 더 높은 비율로 제로 트러스트를 배포하지 않고 있습니다. 이러한 조직에서는 평균 미화 540만 달러의 유출 비용이 발생하였으며, 이는 전 세계 평균보다 100만 달러 이상 높은 액수입니다.

미화 100만 달러

원격 작업이 데이터 유출 요인인 경우와 그렇지 않은 경우 평균 비용 차이

원격 작업이 데이터 유출 요인인 경우, 그렇지 않은 경우에 비해 유출 비용이 평균 거의 미화 100만 달러 가량 더 높았습니다(원격 작업이 요인인 경우 미화 499만 달러, 요인이 아닌 경우 미화 402만 달러). 즉, 원격 작업 관련 데이터 유출 평균 비용은 전 세계 평균에 비해 약 60만 달러가 더 소요된 셈입니다.

45%

클라우드에서 발생한 데이터 유출의 비중

연구 결과, 데이터 유출의 45%가 클라우드에서 발생했습니다. 하지만 하이브리드 클라우드 환경에서 발생한 데이터 유출로 평균 380만 달러의 비용이 소요된 반면, 프라이빗 클라우드에서는 424만 달러, 퍼블릭 클라우드에서는 502만 달러가 소요됐습니다. 하이브리드 클라우드와 퍼블릭 클라우드 사이 데이터 유출로 인한 비용 차이는 27.6%였습니다. 또한 하이브리드 클라우드 모델을 사용하는 조직은 퍼블릭 또는 프라이빗 클라우드 모델을 채택한 조직보다 더 짧은 유출 수명 주기를 나타냈습니다.

미화 266만 달러

인시던트 대응(IR) 팀 및 정기적인 IR 계획 테스트를 통한 평균 비용 절감액

조사 대상 조직의 거의 4분의 3이 IR 계획을 가지고 있었으며, 이 중 63%는 정기적으로 계획을 테스트한다고 응답했습니다. IR 팀을 보유하고 정기적으로 IR 계획을 테스트하는 경우, 상당한 비용 절감 효과를 얻을 수 있었습니다. IR 계획을 테스트하는 IR 팀을 보유한 기업은 그렇지 않은 기업에 비해 평균 266만 달러 낮은 데이터 유출 비용을 나타냈습니다. 이는 592만 달러 대비 326만 달러 차이로, 58%의 비용 절감에 해당합니다.

29일

확장된 탐지 및 대응(XDR) 기술을 사용하는 조직의 대응 시간 단축

조사 대상 조직 중 44%가 XDR 기술을 구현했으며, XDR 기술을 보유한 조직은 대응 시간 면에서 상당한 이점을 얻었습니다. XDR을 배포한 조직은 그렇지 않은 조직에 비해 유출 수명 주기를 평균 한 달 정도 단축했습니다. 특히나 XDR을 배포한 조직은 데이터 유출을 파악하고 억제하는 데 275일이 걸린 반면, 그렇지 않은 조직은 304일이 걸렸습니다. 이는 10%의 대응 시간 차이를 나타냅니다.

12년

의료 업계가 가장 높은 평균 데이터 유출 비용을 기록한 연속 연수

의료 업계의 데이터 유출 비용은 사상 최고치를 경신했습니다. 의료 업계 평균 데이터 유출 비용은 미화 100만 달러 가까이 증가하여, 미화 1,010만 달러에 달합니다. 의료 업계는 2020년 보고서 이후 유출 비용이 41.6% 증가하면서 12년 연속 가장 높은 비용을 지출하였습니다. 금융 기관은 평균 미화 597만 달러로 두 번째 높은 비용을 기록하였습니다. 제약 업계는 미화 501만 달러, 기술 업계는 497만 달러, 에너지 업계는 472만 달러로 그 뒤를 따릅니다.

미화 944만 달러

미국의 평균 데이터 유출 비용(전체 국가 중 최고치)

데이터 유출 평균 비용이 가장 높은 상위 5개 국가와 지역을 살펴보면, 미국 미화 944만 달러, 중동 미화 746만 달러, 캐나다 미화 564만 달러, 영국 미화 505만 달러, 독일 미화 485만 달러에 해당합니다. 미국은 12년 연속 1위를 차지했고, 지난해보다 가장 큰 비용 증가율을 보이는 나라는 브라질로, 미화 108만 달러에서 미화 138만 달러로 27.8% 증가했습니다.

데이터 유출로 인한 재정적 영향을 최소화하기 위한 권장사항

본 섹션에서 IBM Security는 데이터 유출로 인한 재정적 비용과 평판상 피해를 줄이기 위해 조직이 취할 수 있는 조치를 간략히 안내합니다. 이러한 권장사항에는 일부 조사 대상 조직이 성공적으로 실시한 보안 접근 방식을 포함합니다.

제로 트러스트 보안 모델을 채택하여 민감한 데이터에 대한 무단 액세스를 방지하세요.
연구 결과에 따르면, 제로 트러스트 보안 접근 방식을 구현한 조직은 41%에 불과했지만, 완전한 배포로 인해 잠재적으로 미화 150만 달러의 유출 비용을 절감할 수 있었습니다. 여러 조직이 원격 작업과 하이브리드 멀티클라우드 환경을 통합함에 따라, 제로 트러스트 전략을 통해 액세스 가능성을 제한하고 컨텍스트를 요구함으로써 데이터와 리소스를 보호할 수 있습니다.

보안 툴을 사용하여 서로 다른 시스템 간에 데이터를 공유하고 데이터 보안 작업을 중앙 집중화하면, 보안 팀은 복잡한 하이브리드 멀티클라우드 환경 전반에서 인시던트를 탐지할 수 있습니다. 제로 트러스트 전략을 개선할 수 있는 개방형 보안 플랫폼을 통해 더욱 심도 있는 인사이트를 확보하고, 위험을 완화하고, 대응 시간을 단축할 수 있습니다. 이와 동시에 기존에 투자한 인프라를 그대로 활용해 데이터를 그대로 유지할 수 있으므로 팀의 효율성과 협업 기능이 향상됩니다.

정책 및 암호화를 사용해 클라우드 환경에서 민감한 데이터를 보호하세요.
클라우드 환경에서 호스팅되는 데이터의 양과 가치가 증가함에 따라, 조직은 클라우드에서 호스팅된 데이터베이스를 보호하기 위한 조치를 취해야 합니다. 완전한 클라우드 보안 방식을 실행하는 경우, 그렇지 않은 경우에 비해 데이터 유출 비용을 72만 달러 절감하는 효과가 있었습니다. 데이터 분류 스키마와 보존 프로그램을 사용해 가시성을 확보하고 유출에 취약한 민감한 정보량을 감축할 수 있습니다. 데이터 암호화와 완전 동형 암호화를 사용하여 민감한 정보를 보호합니다. 내부 프레임워크를 사용하여 감사 작업을 진행하고, 전사적인 위험을 평가하고, 거버넌스 요구사항의 준수를 추적하면 데이터 유출 탐지 및 억제 능력을 한층 개선 및 강화할 수 있습니다.

보안 오케스트레이션·자동화·대응(SOAR) 및 XDR에 투자해 탐지 및 대응 시간을 개선하세요.
보안 AI 및 자동화와 함께 XDR 기능은 데이터 유출의 평균 비용과 수명 주기를 크게 줄이는 데 도움이 될 수 있습니다. 본 연구에 따르면, XDR을 배포한 조직은 그렇지 않은 조직에 비해 데이터 유출 수명 주기를 평균 29일 단축하고 40만 달러의 비용을 절감했습니다. SOAR, 보안·정보·이벤트 관리(SIEM) 소프트웨어, 관리형 탐지·대응 서비스, XDR은 조직이 자동화, 프로세스 표준화, 기존 보안 툴과의 통합을 통해 인시던트에 신속하게 대응하는 데 도움이 될 수 있습니다.

원격 직원 및 엔드포인트를 모니터링하고 보호하는 데 도움이 되는 툴을 사용하세요.
본 연구에서는 원격 작업이 데이터 유출의 요인인 경우, 그렇지 않은 경우에 비해 거의 미화 100만 달러에 달하는 비용이 더 소요된 것으로 밝혀졌습니다. 통합 엔드포인트 관리(UEM), 엔드포인트 탐지·대응(EDR), ID 및 액세스 관리(IAM) 제품과 서비스는 의심스러운 활동에 대한 더 깊은 가시성을 보안 팀에 제공합니다. 이러한 관리 감독 대상에는 조직이 물리적으로 액세스할 수 없는 엔드포인트를 포함해 BYOD(Bring Your Own Device) 기기, 회사 노트북, 데스크톱, 태블릿, 모바일 기기, IoT 등이 해당합니다. UEM, EDR, IAM은 조사 및 대응 시간을 단축하여, 원격 작업이 데이터 유출의 요인인 경우 유출 피해를 격리하고 억제합니다.

사이버 복원력을 높일 수 있도록 인시던트 대응 플레이북을 생성하고 테스트하세요.
데이터 유출 비용을 완화하는 가장 효과적인 두 가지 방법은 인시던트 대응(IR) 팀을 구성하고 광범위하게 IR 계획을 테스트하는 것입니다. 데이터 유출 발생 시, 정기적으로 IR 계획을 테스트하는 IR 팀이 있는 조직은 그렇지 않은 조직에 비해 266만 달러의 비용을 절감하는 효과를 얻었습니다. 조직은 상세한 사이버 인시던트 플레이북을 작성하여 데이터 유출로 인한 영향을 억제하는 데 신속하게 대응할 수 있습니다. 탁상 훈련을 통해 정기적으로 계획을 테스트하거나, 사이버 레인지와 같은 시뮬레이션 환경에서 데이터 유출 시나리오를 구동합니다.

상대 시뮬레이션 연습은 일명 레드 팀 연습으로도 불리며, IR 팀이 놓칠 수 있는 공격 경로와 기술을 발견하고 탐지·대응 능력의 격차를 파악하여 IR 팀의 효과를 향상시킬 수 있습니다. 공격 표면 관리 솔루션은 실제를 모사한 공격 경험 시뮬레이션을 통해 이전에는 알려지지 않았던 노출 지점을 찾아 보안 상태를 개선하는 데 도움을 줍니다.

보안 실천에 대한 권장사항은 교육 목적으로 제공한 것으로, 결과를 보장하지 않습니다.

Ponemon Institute / IBM Security 소개

Ponemon Institute

Ponemon Institute는 기업과 정부 내에서 정보·프라이버시에 대한 책임 있는 관리 방식을 발전시키는 독립적인 연구 및 교육에 전념하고 있습니다. 사람 및 조직에 대한 민감한 정보의 보안과 관리에 영향을 미치는 중요 문제를 다루며 수준 높은 실증 연구를 수행하는 것이 본 연구소의 사명입니다.

Ponemon Institute는 엄격한 데이터 기밀 유지, 프라이버시 및 윤리적인 연구 기준을 준수합니다. 개인을 대상으로 어떠한 개인 식별 정보도 수집하지 않으며, 또한 기업 연구 시 기업 식별 정보를 수집하지 않습니다. 아울러, 엄격한 품질 기준에 따라 연구 대상자에게 연구 주제를 벗어나거나, 연구와 관련이 없거나, 부적절한 질문을 하지 않습니다.

IBM Security

IBM Security는 기업용 보안 제품과 서비스에 대한 최고급 통합형 포트폴리오를 제공합니다. 세계적인 명성을 자랑하는 IBM Security X-Force® 연구가 뒷받침된 이 포트폴리오는 조직의 비즈니스 패브릭에 보안을 적용하도록 보안 솔루션을 제공하여, 불확실한 상황에도 조직이 성공적으로 비즈니스를 이어갈 수 있도록 지원합니다.

IBM은 최고 수준의 광범위하고 심층적인 보안 연구, 개발, 제공 조직을 운영하고 있습니다. IBM은 전 세계 130개 이상의 국가에서 매월 4조 7천억 건 이상의 이벤트를 모니터링하고, 1만 개가 넘는 보안 특허를 보유하고 있습니다. 더 자세한 내용은 ibm.com/kr-ko/security를 방문하세요. 또한 IBM Security Community에서 함께 이야기를 나누어 보세요.

보고서 인용 또는 복제 허가를 비롯한 본 연구 보고서에 대한 질문이나 의견이 있으신 경우, 우편, 유선 전화 또는 이메일로 문의하시기 바랍니다.

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

1.800.887.3118
research@ponemon.org

다음 단계 안내

제로 트러스트 보안 솔루션
모든 사용자, 디바이스, 연결에 엄격한 보안을 적용하세요.
더 알아보기

ID 및 액세스 관리
모든 사용자, API, 디바이스를 모든 앱에 안전하게 연결하세요.
더 알아보기

데이터 보안
민감한 기업 데이터를 검색하고, 분류하고, 보호하세요.
더 알아보기

보안 오케스트레이션, 자동화, 대응
보안 오케스트레이션 및 자동화를 통해 인시던트 대응 시간을 단축하세요.
더 알아보기

보안 정보 및 이벤트 관리
위협을 탐지하고, 조사하고, 대응할 수 있는 가시성을 확보하세요.
더 알아보기

클라우드 보안
귀사의 하이브리드 멀티 클라우드 여정에 보안을 통합하세요.
더 알아보기

엔드포인트 보안
지능형 공격으로부터 디바이스, 사용자, 조직을 보호하세요.
더 알아보기

사이버 보안 서비스
컨설팅, 클라우드, 관리형 보안 서비스를 통해 위험를 줄이세요.
더 알아보기

인시던트 대응 및 위협 인텔리전스
선제적으로 보안 위협을 관리하고 대응하세요.
더 알아보기

IBM Security X-Force 전문가와 일대일 상담을 예약하세요.
지금 예약하기

(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)

미국에서 제작됨
2022년 7월