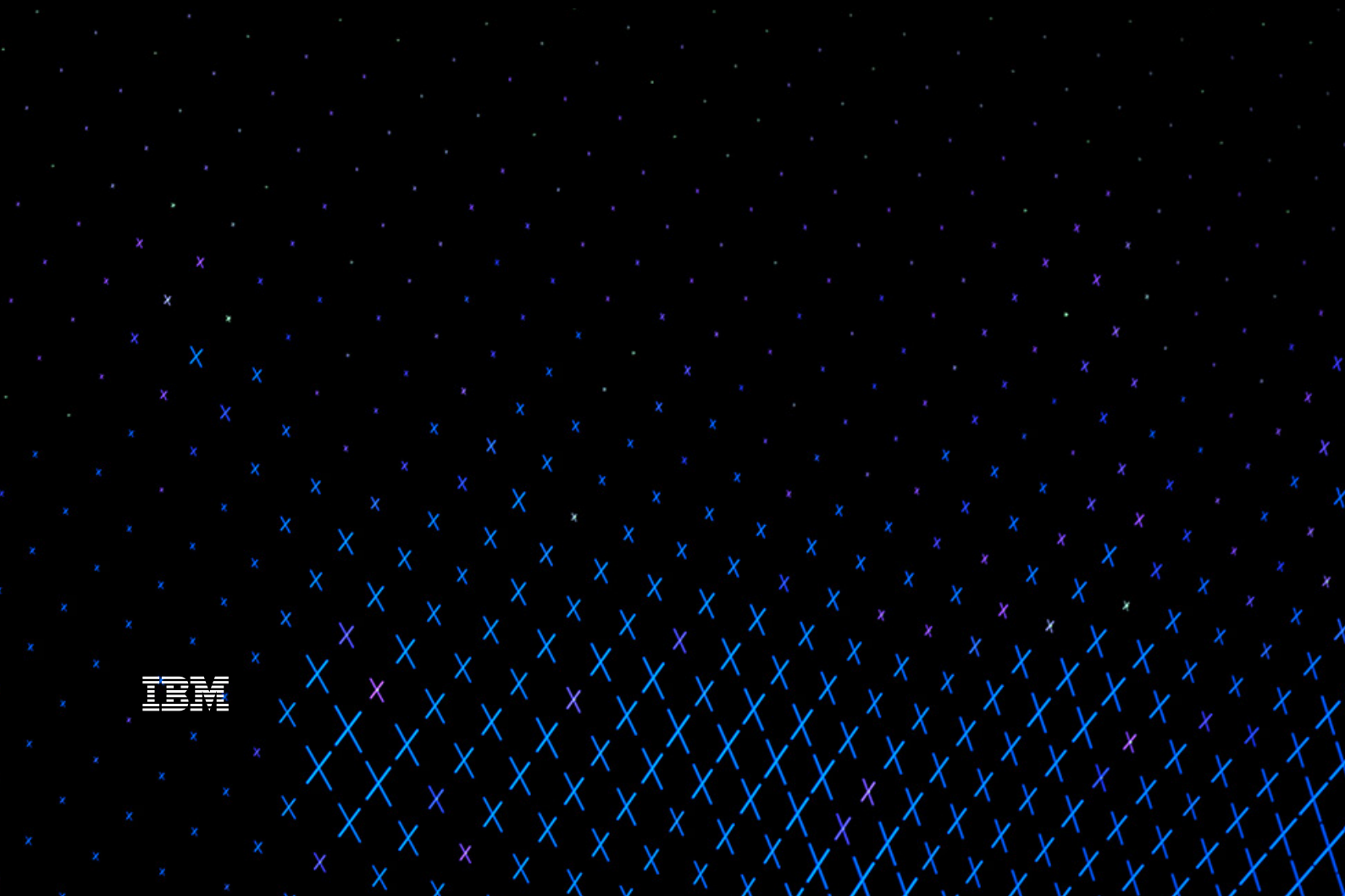
IBM Security

사이버 복원력 우수 조직 보고서 2020



IBM

목차

개요

올해로 5회째를 맞이한 IBM Security의 *사이버 복원력 우수 조직 보고서* 는 2020년 4월 3,400 명이 넘는 전 세계 IT 및 보안 전문가를 대상으로 설문조사를 실시하여 사이버 보안 인시던트를 탐지, 방지, 확산 저지 및 대응하는 조직의 역량을 평가한 Ponemon Institute의 연구 결과를 바탕으로 합니다.

사이버 보안 인시던트의 양이 급격히 증가하여 IT와 비즈니스 프로세스에 심각한 장애를 일으키고 있습니다. 동시에 높은 수준의 사이버 복원력을 실현했다고 대답한 조직의 비율이 2015년 35%에서 2020년 53%로 증가했습니다. 사이버 복원력 우수 조직이란 데이터와 애플리케이션, IT 인프라를 공격하는 다양한 위협을 보다 효과적으로 방지, 탐지, 확산 저지하고 대응하는 조직으로 정의할 수 있습니다.

현재 응답자의 1/4 이상이 일관성 있는 전사적 사이버 보안 인시던트 대응 계획(CyberSecurity Incident Response Plan, CSIRP)을 기반으로 사이버 복원력을 보장하고 있습니다. 대부분의 조직은 자사의 보안 환경을 공고히 하기 위해 자동화, 머신러닝, AI, 클라우드, 조정 등 첨단 기술을 이용합니다.

하지만 자원과 예산의 제약, 갈수록 정교해지는 위협과 IT 환경의 복잡성에서 보안 팀의 사이버 공격 저지 역량 저하까지 아직 풀어야 할 숙제들이 남아 있습니다.

본 보고서에서는 사이버 복원력을 전반적으로 개선하기 위해 조직이 이용하는 접근 방법과 우수 사례를 소개합니다. 또한 사이버 공격 발생 시 비즈니스 중단을 최소화하기 위해 강력한 보안 태세 구축에서 사이버 복원력의 중요성에 대해 자세히 설명합니다. 마지막으로, 사이버 복원력이 뛰어난 조직으로 탈바꿈하는 데 도움이 되는 권장 사항을 제시해 줍니다.

사이버 복원력 우수 조직 보고서에 담긴 사실

51%

지난 2년 동안 사이버 보안 인시던트로 인해 **중대한 비즈니스 장애** 를 보고한 조직의 비율

26%

전사적 CSIRP를 사용하는 조직의 비율

55%

자동화 도구를 통한 **사이버 복원력 개선** 을 보고한 우수 조직의 비율

52%

클라우드 서비스를 통해 사이버 복원력이 개선되었다고 대답한 응답자의 비율

45

사용 중인 **보안 솔루션** 과**기술** 의 평균 개수

2020년의 새로운 보고서 사항

올해의 보고서에는 끊임없이 변화하는 보안 환경에 대응하기 위해 클라우드 서비스 사용이 조직의 사이버 복원력에 어떤 개선 효과를 가져오고 주요 이점은 무엇인지에 대해 최초로 조사한 내용이 담겨 있습니다. 또한 멀웨어, 피싱 같은 일반적인 보안 공격을 해결하기 위한 조직의 대응 계획 사용 실태에 관한 질문도 추가로 담겨 있습니다.

보안 인시던트를 조사하고 대응하는 데 사용되는 도구의 수에 대한 이해를 높이고자 지난해 조사한 보안 솔루션의 수에 관한 질문에서 확장한 것입니다.

IBM은 작년과 비슷하게, 수준 높은 사이버 복원력을 구축한 조직을 "우수 조직" 등으로 분류하고 차별화 요소를 연구하여 사이버 복원력 측정을 위한 벤치마크를 마련했습니다. 본 보고서에서는 자동화 도구와 클라우드 서비스를 이용하고, 상호 운용성에 주력하는 등 우수 조직이 사이버 복원력 수준을 강화할 수 있었던 전술을 집중적으로 설명합니다.

주요 결과

CSIRP를 수립한 조직은 비즈니스 장애 횟수가 감소했습니다.

사이버 복원력 인시던트 대응 계획(CSIRP)이 비즈니스 장애를 최소화합니다.

전사적 CSIRP 도입이 2015년 이후 느린 속도로 향상되어 44% 증가했습니다. 이러한 결과와 이점에도 불구하고 응답자의 51%는 자사의 CSIRP가 기업 전체에 일관적으로 적용되고 있지 않거나, 임시 계획이거나 비공식적인 계획일 뿐이라고 답변했습니다.

공식 CSIRP를 수립한 조직 중에서도 DDoS 또는 멀웨어 같은 일반적인 공격에 대비해 공격별 플레이북을 마련해 놓은 조직이 3분의 1에 불과합니다. 랜섬웨어와 같은 새로 등장한 위협 관련 계획이 수립되어 있다고 답변한 응답자는 거의 없었습니다.

뿐만 아니라 7%의 조직만 분기마다 CSIRP를 검토하는데, 지난 5년 동안 이 수치는 크게 달라진 점이 없습니다. 사실 정기적으로 계획을 검토하고 업데이트하지 않는 조직이 전체의 40%에 달하며 이는 2015년 이후 8% 증가한 수치입니다. 기업 전체에 적용되는 최신 CSIRP의 부재로 더 많은 조직이 IT 및 비즈니스 프로세스의 중대한 장애를 경험했습니다.

모든 공격을 저지하는 것은 불가능하겠지만 효과적인 준비와 대응 절차를 마련한다면 피해를 대폭 줄일 수 있을 것입니다. 본 조사에서 드러났듯이 CSIRP에 대한 관심과 노력 부족이 공격적인 위협 환경에서 대응 효과를 제한하는 원인이 되고 있습니다.

-8%

사이버 공격 탐지 역량에서 **50개 이상 도구를** 사용하는 조직은 그 순위가 **8% 낮게** 평가되었습니다.

너무 많은 도구는 사이버 복원력을 약화시키고 자동화, 가시성, 상호 운용성은 인시던트 대응을 개선합니다.

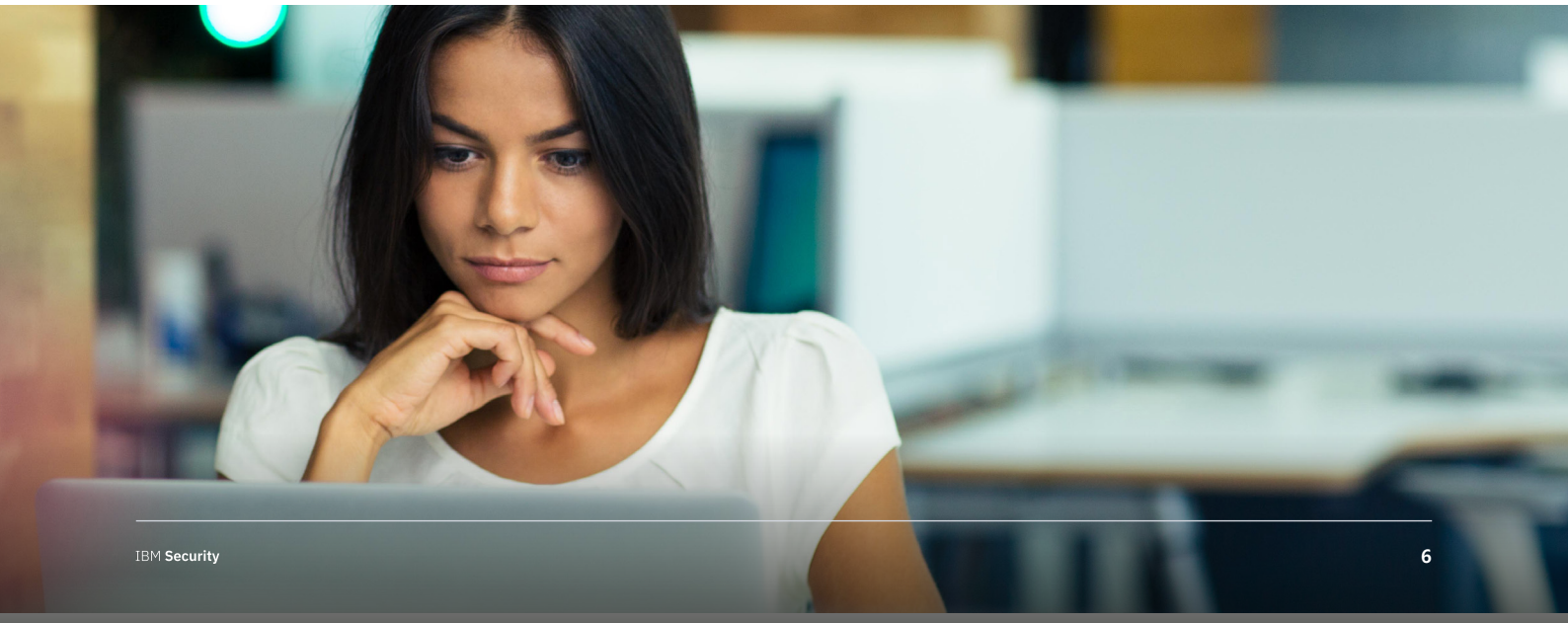
조직은 보안 환경을 관리하고 사이버 보안 인시던트에 대응하기 위해 수많은 도구를 사용했습니다. 30%에 가까운 조직이 50가지 이상의 보안 솔루션과 기술을 사용하고, 45%는 사이버 보안 인시던트를 전문적으로 조사하고 대응할 때 20가지가 넘는 도구를 사용했습니다.

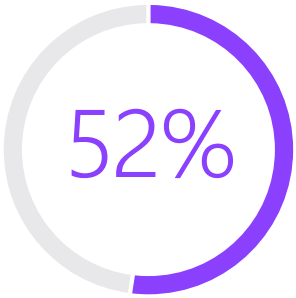
하지만 상호 연결되지 않은 도구의 과도한 사용은 복잡한 환경과 효율성 저해를 초래합니다. 이번 조사에서 조직이 사용한 보안 솔루션과 기술의 수가 사이버 보안 인시던트를 탐지, 방지, 확산 저지, 대응하는 역량에 부정적인 영향을 미치는 것으로 나타났습니다.

사실 50개 미만의 도구를 사용하는 회사에 비해 50개 이상의 도구를 사용하는 회사는 사이버 공격 탐지 역량 부문에서 순위가 8% 더 낮았고 공격 대응 역량 부문에서 7% 더 낮았습니다.

애플리케이션과 데이터를 파악하는 가시성이 지난 3년 동안 조직의 사이버 복원력 개선을 주도한 효과적인 방법 중 하나였습니다. 특히 올해에는 우수 조직에서 주목 받는 또 다른 이유로 자동화가 대두되고 있습니다. 상호 운용 가능한 도구의 사용이 사이버 복원력 개선에 도움이 되었다고 답변한 우수 조직은 63%인 반면 비우수 조직은 46%입니다.

이와 같이 상호 운용성에 중점을 두면서 다수 공급업체의 솔루션을 도입할 수 밖에 없는 요즘 시대에 절실하게 요구되는 포괄적인 가시성을 확보하고 복잡성도 완화할 수 있었습니다.





클라우드 서비스로 사이버 복원력이 개선되었다고 답변한 응답자의 수

클라우드 서비스는 사이버 복원력을 강화시켜 줍니다.

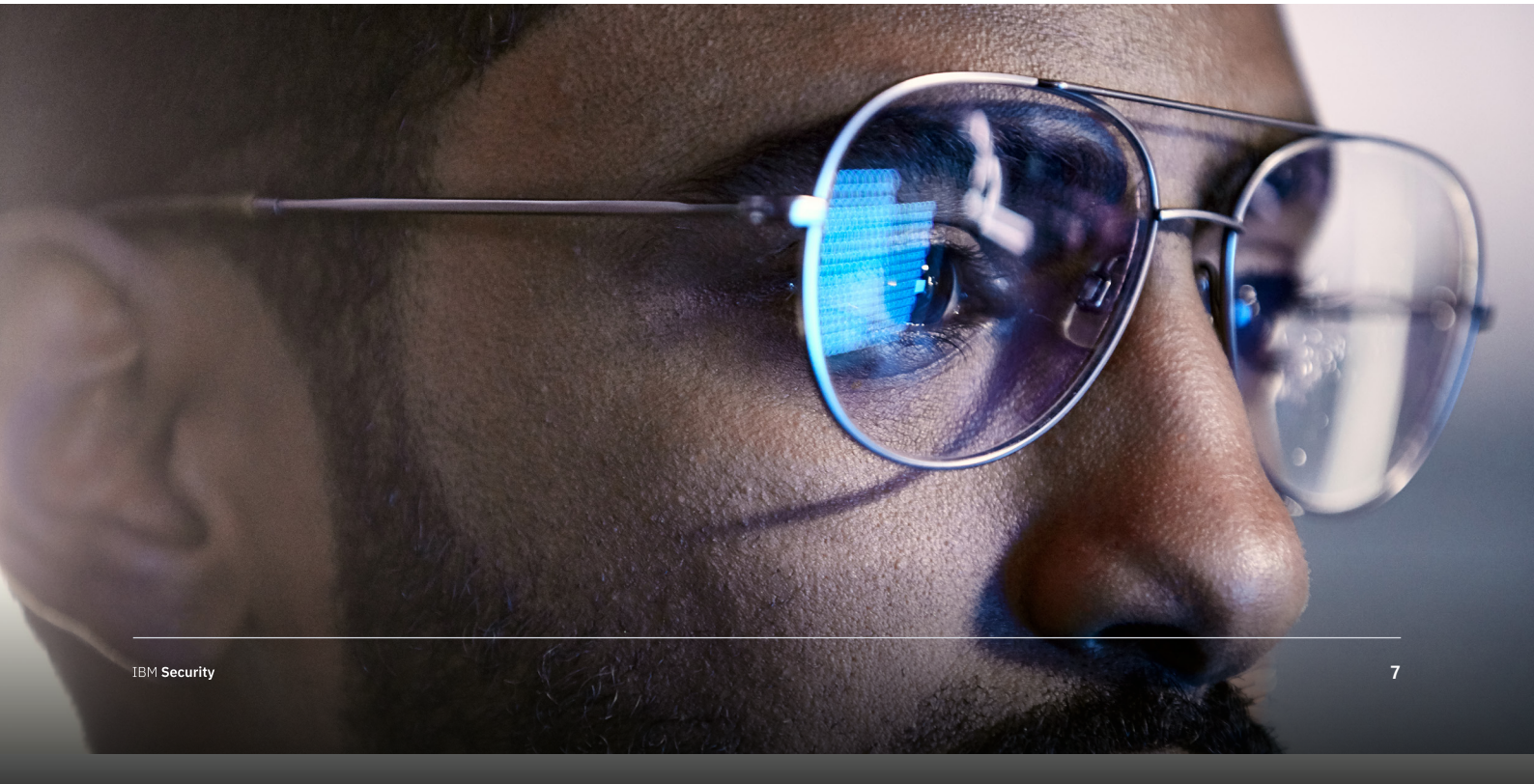
전체 응답자의 52%가 클라우드 서비스의 사용으로 사이버 복원력이 개선되었다고 답변했습니다. 우수 조직만 따로 구분해서 보면 클라우드 서비스 사용이 사이버 복원력을 개선하고 있다고 응답한 비율이 비우수 조직의 49%에 비해 63%를 차지합니다.

클라우드를 조기 도입한 금융 서비스 조직의 60%가 클라우드 서비스 사용이 조직의 사이버 복원력 개선에 효과적으로 작용했다고 답변한 것은 놀라운 일이 아닙니다. 의료 및 소매 조직과 공공 부문 역시 클라우드 서비스 도입으로 이전 사례와 비슷한 개선 효과를 보고합니다.

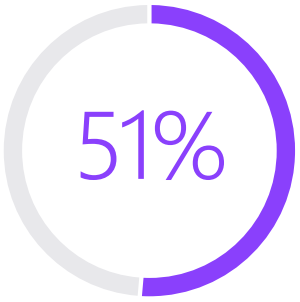
영국, 독일, 프랑스, 미국, 캐나다 소재 회사들을 주축으로 사이버 복원력 실현에서 클라우드 서비스의 가치와 중요성을 높이 평가하는 의견이 나왔습니다. 특히, 이들 국가에 존재하는 조직의 3분의 2 이상이 클라우드 서비스의 가치를 인정하고 있습니다.

우수 조직에 따르면 클라우드 서비스를 통해 사이버 복원력이 개선되는 주된 이유는 분산 환경과 규모의 경제를 이용하고 서비스 수준 계약을 보장받을 때 얻을 수 있는 이점 때문이었습니다. 한편 30%의 조직은 비효율적으로 구성된 클라우드 서비스가 사이버 복원력 개선에 방해가 되었다고 답변했습니다.

효과적인 환경을 구축하기 위해서는 클라우드 서비스 투자만으로 충분하지 않고 최적화가 반드시 이루어져야 합니다.



유용한 추가 정보

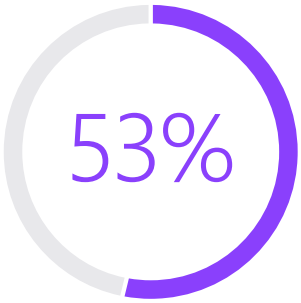


지난 2년 동안 **사이버 공격으로 심각한 타격을** 입은 조직의 수

사이버 공격의 양과 심각도가 증가했습니다.

설문조사에 응한 조직의 대다수(53%)는 지난 2년 동안 민감한 데이터나 고객 또는 비즈니스 관련 기밀 정보가 저장된 1,000개 이상의 기록이 손실되거나 탈취되는 데이터 유출을 경험한 적이 있습니다. 비슷한 숫자(51%)가 지난 2년 동안 조직의 IT 및 비즈니스 프로세스에 중대한 장애를 유발한 사이버 보안 인시던트를 보고했습니다.

67%와 64%는 공격의 양과 심각도가 각각 지난 12개월 동안 크게 증가했다고 말했습니다. 심각도의 주요 측정 기준은 중요한 정보 자산의 유출(57%)과 직원 생산성 저하(50%)입니다.



사이버 복원력이 개선된 조직의 수

사이버 복원력은 전반적으로 향상된 반면, 지난 5년 동안 가장 개선된 부분은 공격 방지 역량입니다.

지난 5년 동안 조직의 사이버 복원력 수준이 급격히 발전하여 51%의 개선이 보고되었습니다. 이러한 상승 효과는 사이버 공격 방지 역량의 현저한 강화와 맞물리면서 2015년 38%에서 2020년 53%까지 향상되었습니다.

사실, 대다수 조직(56%)은 사이버 공격 방지 횟수를 기준으로 사이버 복원력의 개선 정도를 측정합니다. 사이버 복원력의 개선 정도를 측정하는 그 외 주요 지표에는 인시던트 확산 저지 시간 그리고 직원 생산성 향상이 있습니다.

사이버 복원력을 벤치마킹할 때 자주 사용되는(51%) 또 다른 방법인 공격 탐지 역량은 2015년 이후 다소(11%) 개선되었습니다. 대응 역량은 정체되어 있고, 확산 저지 역량은 응답자들이 관련 부분의 13% 감소를 언급하며 점점 더 까다로워지고 있는 것으로 나타났습니다.

사이버 보안 인시던트 대응 계획(CSIRP)을 마련한 조직이 77%에 달하지만 이 계획을 기업 전체에 적용하는 기업은 26%에 불과한 점을 감안하면 이와 같은 쇠퇴는 놀라운 일이 아닙니다. 더욱이 77% 조직 중 4분의 1은 자사의 CSIRP가 비공식적 계획 또는 임시 계획이라고 말했습니다.

<50%

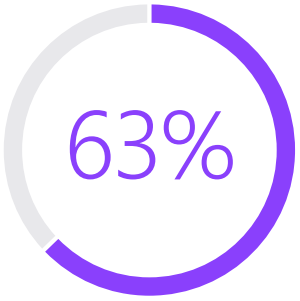
C-레벨 임원/이사진에 사이버 복원력을 보고하는 조직

예산 및 기술 부족은 여전히 강력한 사이버 복원력을 가로막는 문제입니다.

예측한 대로 유능한 기술 인력의 손실(41%)과 예산 부족(40%)이 미흡한 개선의 주요 원인입니다. 응답자들이 강력한 보안 태세 구축의 열쇠로 기술을 꼽는 만큼 많은 조직이 최신 도구를 배포하고 현재 가진 도구를 최대한 활용하기 위해 노력하고 있습니다.

하지만 사일로 및 각 부서간 문제(31%), 자동화(25%), 단편적인 IT 및 보안 인프라(22%)와 같은 앞선 기술의 부족 등 풀어야 할 숙제가 만만치 않습니다.

놀랍게도 응답자의 45%만이 사이버 복원력 실태를 경영진이나 이사회에 공식 보고하고 있다고 대답했습니다. 하지만 사이버 보안 기능에 대한 경영진의 이해와 지지, 이사회 보고는 사이버 복원력이 개선되지 않은 이유 중 가장 중요도가 낮은 요인으로 평가되었습니다.

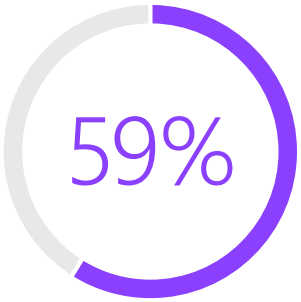


자동화, 머신러닝, AI, 조정이 사이버 복원력을 개선 해 준다고 **대답한 조직의 수**

분석, 자동화, AI 및 머신러닝이 보안 태세를 강화합니다.

응답자들은 분석(46%), 자동화(42%), AI 및 머신러닝(41%)과 같은 기술을 구현한 후 사이버 복원력이 개선되었다고 대답했습니다.

전반적으로, 63% 조직이 사이버 복원력 보안 태세를 강화해준 요인으로 이러한 도구들을 꼽았고 그 뒤를 이어 강력한 개인정보 보호 요건(60%)을 지목했습니다. 본 보고서 뒷부분에서 살펴보겠지만 기술이 사이버 복원력 우수 조직과 그렇지 못한 조직을 가르는 중요한 차이점으로 드러났습니다.

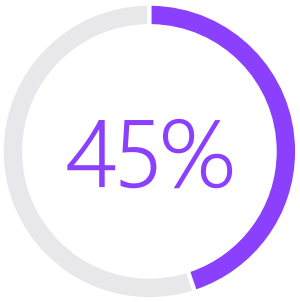


위협 인텔리전스 공유로 사이버 복원력이 개선되었다고 대답한 조직의 수

위협 인텔리전스를 공유할 때의 주된 이점은 협업 환경 조성입니다.

응답자의 59%는 위협 인텔리전스를 공유하면 사이버 복원력이 개선된다는 믿음을 갖고 있었습니다. 협업 환경을 조성하기 위해 57%의 조직이 사이버 위협과 취약점에 대한 정보를 정부 및/또는 업계 다른 회사와 공유하는 프로그램 또는 이니셔티브에 참여하고 있습니다.

사이버 위협 정보를 공유하지 않는 이유를 묻는 질문에 응답자들은 조직에 피부로 와닿는 이점이 없음(70%), 인력 부족(58%), 비용(54%) 등을 가장 많이 꼽았습니다.



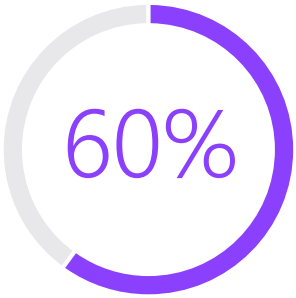
랜섬웨어 공격 대비 계획이 마련되지 않은 조직의 수

DDoS는 가장 일반적인 공격별 대응 계획입니다.

공격 유형별 대응 계획의 사용 여부를 묻는 설문조사가 처음으로 진행되었습니다. 가장 일반적으로 사용되는 계획은 분산 서비스 거부(DDoS), 멀웨어(스파이웨어, 바이러스, 트로이 목마, 웜), 내부자 인시던트, 피싱이었습니다.

공격 계획 사용은 산업별로 차이가 있었습니다. 멀웨어는 공공 부문, 소매, 제조, 소비자 제품 등의 업종에서 가장 많이 사용되는 대응 계획이고, 내부자 인시던트 대응 계획은 산업 환경에서 광범위하게 사용되었습니다. 그 외 업종은 가장 널리 사용되는 계획으로 DDoS를 꼽았습니다.

공격별 플레이북을 사용하는 조직 중에서 랜섬웨어 공격 대비 계획을 수립해 놓은 비율은 절반이 채 되지 않았습니다(45%). 2020년 X-Force Threat Index에 따르면 랜섬웨어는 최근 70% 가까이 급증한 위협 요소입니다. *X-Force Threat Index*. CSIRP를 자주 업데이트하지 않는 조직이 대부분이므로 이러한 주요 위험 영역에 대한 계획의 부재는 계획을 자주 검토하고 최신 공격 기법이 반영되도록 업데이트해야 하는 중요성을 한번 더 부각시켜 줍니다.



사이버 복원력 실현을 위해 **강력한 개인정보 보호 요건이 중요하다고** 대답한 응답자의 비율

개인정보 보호는 사이버 복원력의 필수 요소입니다.

지난 2년 동안 53%의 조직이 민감한 데이터나 기밀 정보가 저장된 1,000개 이상의 기록이 탈취되는 데이터 유출 사고로 피해를 경험한 상황에서 응답자의 95%가 고객 및 직원 데이터 보호 업무를 맡고 있는 개인정보 보호 담당자의 중요성을 인식하는 있는 점은 그리 놀라운 일이 아닙니다.

하지만 3분의 1 이상이 개인정보 보호 담당자를 필수 역할이라고 생각하는 반면 조직의 사이버 복원력 강화 노력을 책임지고 주도하는 개인정보 보호 책임자를 임명한 조직은 1%에 불과합니다. 22%는 비즈니스 사업부 책임자 또는 CIO가 해당 역할을 맡고 있다고 대답했습니다.

응답자의 60%는 2019년과 마찬가지로 "강력한 개인정보 보호 요건"이 사이버 복원력을 실현하는 데 매우 중요하다고 말했습니다. 57%는 EU의 GDPR (개인정보 보호법)과 캘리포니아 소비자 개인정보 보호법(CCPA) 같은 데이터 보호 규정을 준수하는 것이 사이버 복원력을 실현하는 데 중요한 역할을 한다고 언급했습니다.

사이버 복원력 우수 조직의 차별화 요소

자사의 사이버 복원력 수준을 10점 만점을 기준으로 1~10점의 점수로 평가해 달라는 요청에 응답자의 4분의 1 가량이 9점 이상을 주었습니다. 해당 그룹 중 59%는 지난해 조직의 사이버 복원력이 현저하게 개선되었다고 대답했습니다. IBM은 이러한 조직을 사이버 복원력 우수 조직이라고 부릅니다.

작년과 비슷하게 이들 우수 조직은 사이버 공격의 방지, 탐지, 확산 저지, 대응 역량에서 다른 조직들을 앞서는 결과를 보였으며 올해에는 그 차이가 훨씬 커졌습니다. 가장 큰 차이점은 공격을 확산 저지하고 대응하는 역량입니다.

공격 확산을 저지할 때 우수 조직과 다른 조직의 역량 차이가 지난해 14%였던 반면 올해에는 35%로 증가했습니다. 마찬가지로 지난해 사이버 공격 대응 부문에서 우수 조직과 그렇지 못한 조직의 차이는 15%였고, 2020년에는 그 차이가 31%입니다.

분명한 점은, 우수 조직은 비우수 조직들이 배울 만한 효과적인 방법들을 이용하고 있다는 사실입니다. 사이버 복원력 우수 조직의 특징과 접근 방법은 다음과 같습니다.

전사적 CSIRP 구현:

사이버 복원력 우수 조직의 43%는 전사적 CSIRP를 일관되게 적용하고 있는 반면, 비우수 조직은 20%에 불과합니다. 분기마다 또는 한해 2회에 걸쳐 이 계획을 검토하고 테스트하는 우수 조직 비율이 두 배 이상 많습니다.

공격별 대응 계획 사용:

공격별 대응 계획을 사용하는 비율이 40%인 반면 비우수 조직은 37%입니다.

기술 투자:

73%가 자동화, 머신러닝, AI 및 조정을 강력한 사이버 복원력 보안 태세를 실현하기 위해 핵심 요소로 여기는 반면 비우수 조직은 60%입니다.

적극적인 자동화 사용:

70%가 자동화를 적극 사용하거나 적당히 사용한다고 대답했습니다. 이들 그룹 중:

— 70%는 자동화를 통해 운영 효율성을 개선했습니다.
— 64%는 자동화를 사용하여 IT 보안 팀을 지원했습니다.

위협 인텔리전스 공유:

69%가 위협 인텔리전스 공유로 사이버 위협을 탐지, 확산 저지, 대응하는 역량을 개선하는 데 도움이 되었다고 대답한 반면 비우수 조직은 50%입니다.

C-레벨 임원의 가시성:

우수 조직의 절반 이상이 C-레벨 경영진 및/또는 이사진에 공식 보고합니다.

우수 조직과 비우수 조직 비교

39%
자동화 도구를 통해 개선 효과를 실현한 적이 더 많음

25%
클라우드 서비스를 배포하여 개선한 적이 더 많음

20%
AI와 머신러닝을 사용하여 개선 효과를 경험한 적이 더 많음

31%
상호 운용 가능한 사이버 보안 도구를 통해 개선 효과를 실현한 적이 더 많음

사이버 복원력 개선 조치*

전사적 CSIRP를 구현하여 비즈니스 장애를 최소화합니다.

CSIRP를 수립하는 것만으로 충분하지 않고 조직 전체에 구현한 후 정기적으로 검토해야 합니다. 해마다 공격의 양과 심각도가 증가하면서 업데이트된 CSIRP의 부재가 IT 및 비즈니스 프로세스에 심각한 장애를 초래할 위험이 커질 수 있습니다.

업종별 공격에 맞게 대응 계획을 조정합니다.

사이버 보안 공격은 다양한 형태로 나타납니다. 조직은 자사 업종의 가장 중요한 위협을 이해하고 세부 대응 계획을 준비하여 보안 태세를 강화하는 동시에 팀원이 특정 공격을 조사 및 해결하는 데 필요한 조치를 확실하게 숙지할 수 있도록 지원해야 합니다.

상호 운용성을 수용하여 가시성을 높이고 복잡성을 최소화합니다.

조직이 복잡한 보안 환경을 전반적으로 탐색하고, 가장 효율적인 팀이 상호 운용성을 기반으로 공격을 방지 및 탐지하는 데 활용되는 도구와 데이터의 가시성을 높입니다. 워크플로우를 능률화하는 접근 방법은 보안 관제 센터의 생산성을 높이는 데 도움이 됩니다.

기술에 투자하여 인시던트 대응을 가속화합니다.

자동화, 분석, AI, 머신러닝과 클라우드 서비스 등의 기술은 조직이 사이버 복원력을 개선할 수 있었던 주된 이유였습니다. 특히 자동화는 운영 효율성을 개선하고 조사와 대응에 필요한 중요 업무에 주력할 시간적 여유를 주어 팀의 업무 집중도를 높이는 데 큰 역할을 하고 있습니다.

*보안 관행에 관한 권한사항은 교육 목적으로 제공되며 특정 결과를 보장하지 않습니다.

보안 팀과 개인정보 보호 팀의 협업을 이끌어냅니다.

사이버 복원력이 우수한 조직은 보안과 개인정보 보호가 일맥상통한다는 점을 인식하고 있습니다. 사일로를 없애고 협업 문화를 조성하여 데이터 유출에 보다 효과적으로 대응하십시오. 보안 팀과 개인정보 보호 팀의 협업이 조기에 원활하게 이루어진다면 대규모 보안 인시던트 발생 시 처음 협력하는 경우보다 빠르게 보안 태세를 개선할 수 있게 됩니다.

조직 사이버 복원력에 대한 가시성 향상을 위해 C-레벨 임원/이사회를 상대로 한 보고를 공식화합니다.

비즈니스 리더들은 사이버 복원력이 기업의 수익과 평판에 큰 영향을 미치므로 필요한 투자와 자원을 확보하기 위해 사이버 복원력 성과를 최우선 과제로 삼아야 한다는 점을 잘 알고 있습니다.

전체 결과

그림 1

사이버 보안 인시던트를 경험한 조직의 수

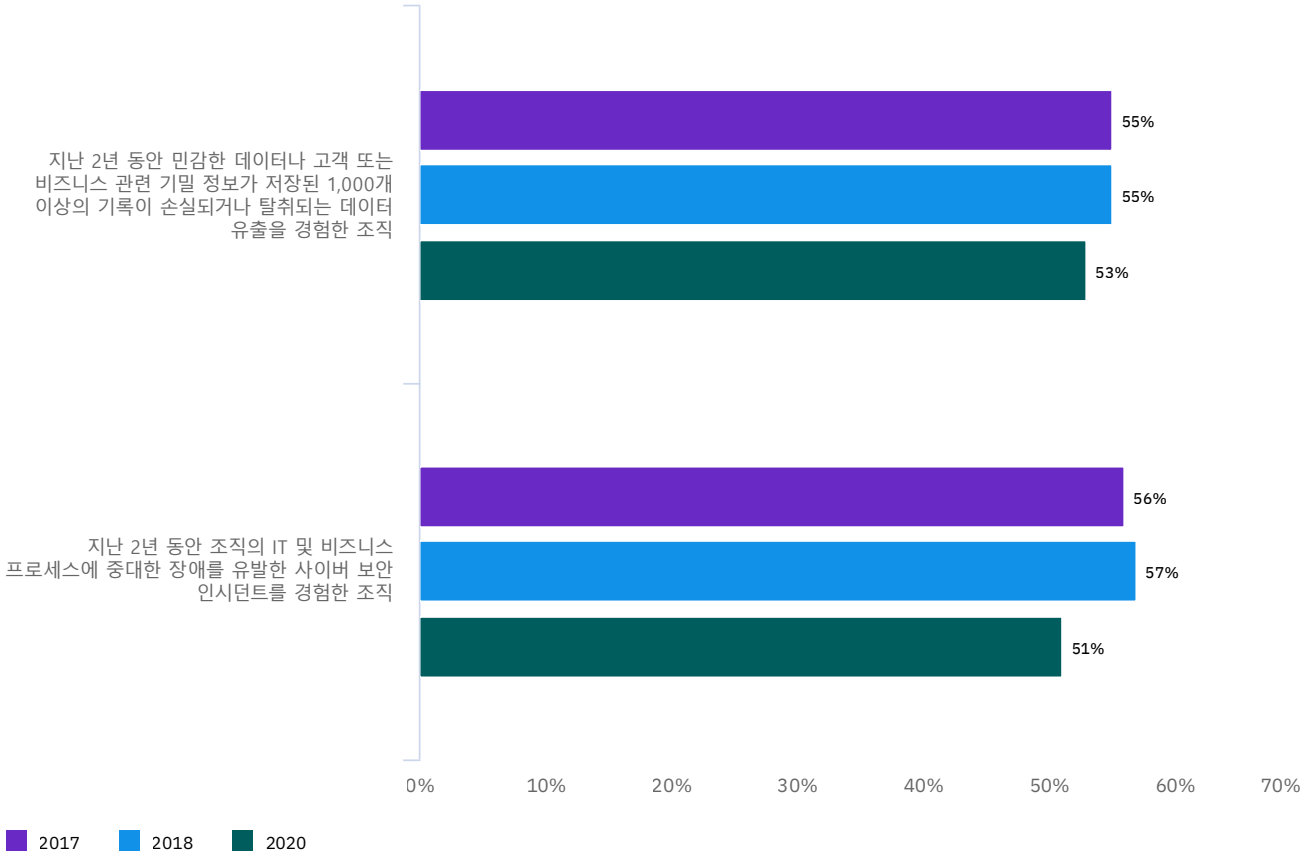


그림 1 은 지난 2년 동안 데이터 유출 또는 사이버 보안 인시던트를 경험한 적이 있는 조직의 수를 보여줍니다.

그림 2

개선 정도 측정 기준

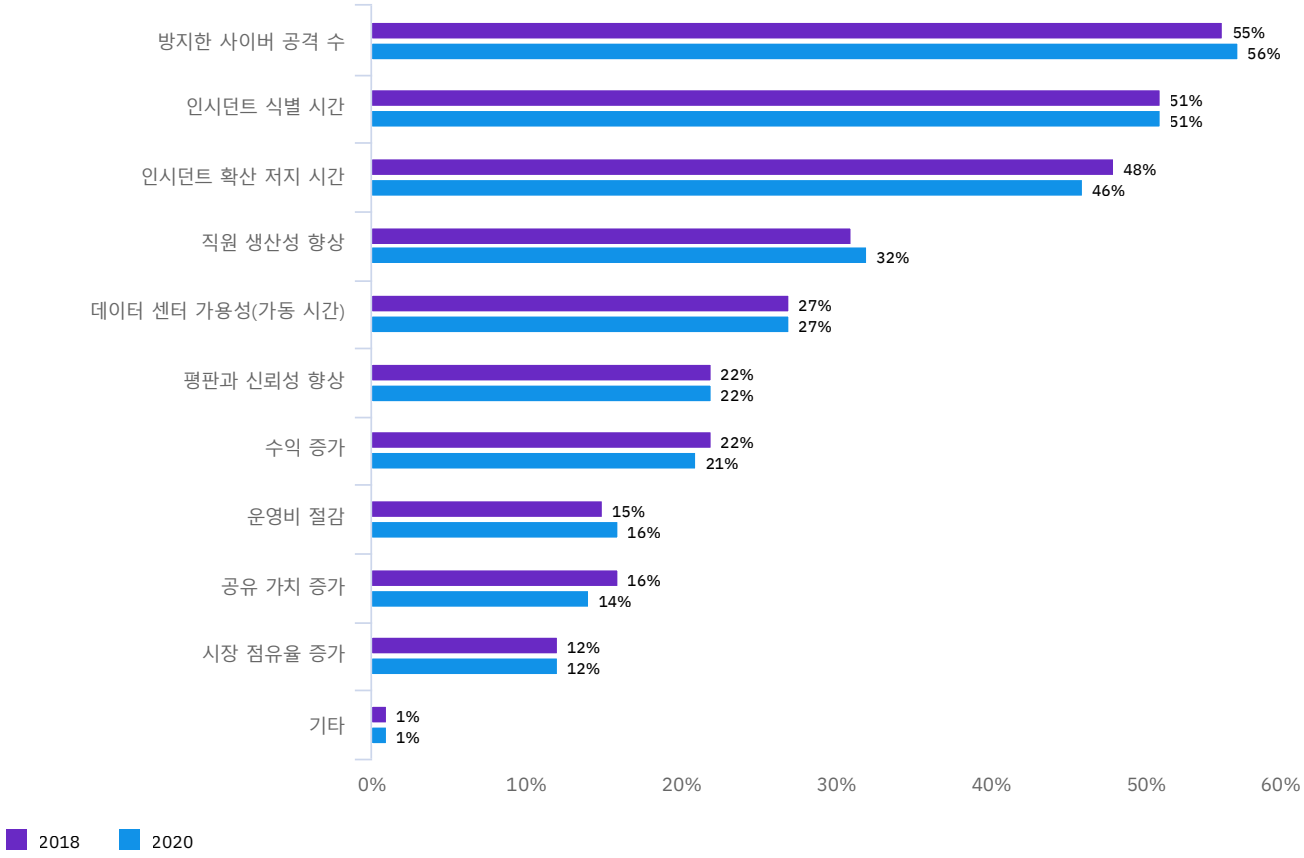


그림 2 는 사이버 복원력의 개선 정도를 측정하는 척도에 대한 유용한 정보를 제공합니다. 10개 요소 중 상위 3개 요소는 방지한 사이버 공격 수, 인시던트 식별 시간, 인시던트 확산 저지 시간입니다.

그림 3

사이버 복원력이 개선된 이유

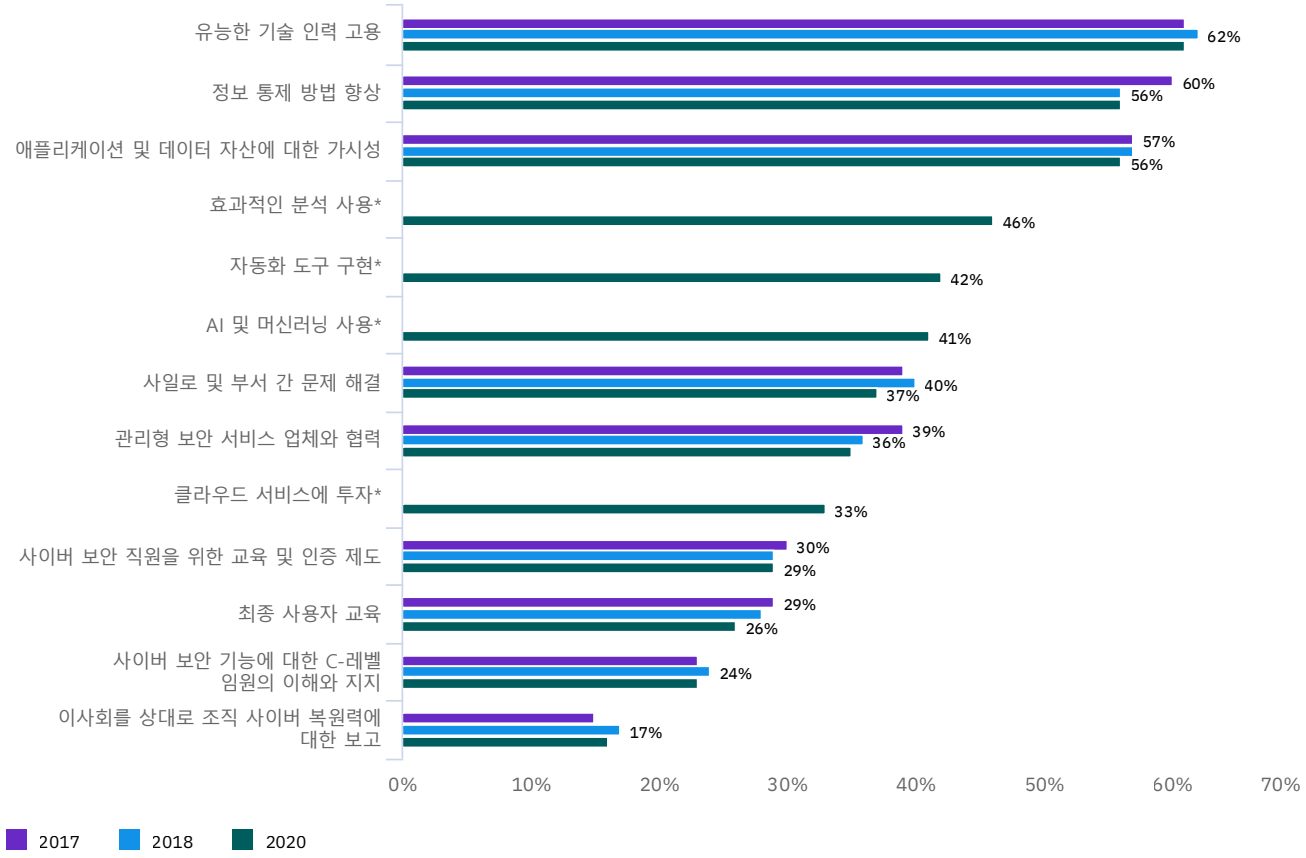


그림 3 은 조직이 사이버 복원력이 개선될 수 있었던 이유를 보여줍니다. 상위 3개 요소는 매해 크게 달라지지 않는 반면 올해는 분석, 자동화, AI 및 머신러닝이 눈에 띄는 역할을 했습니다.

그림 4

사이버 복원력이 개선되지 않은 이유

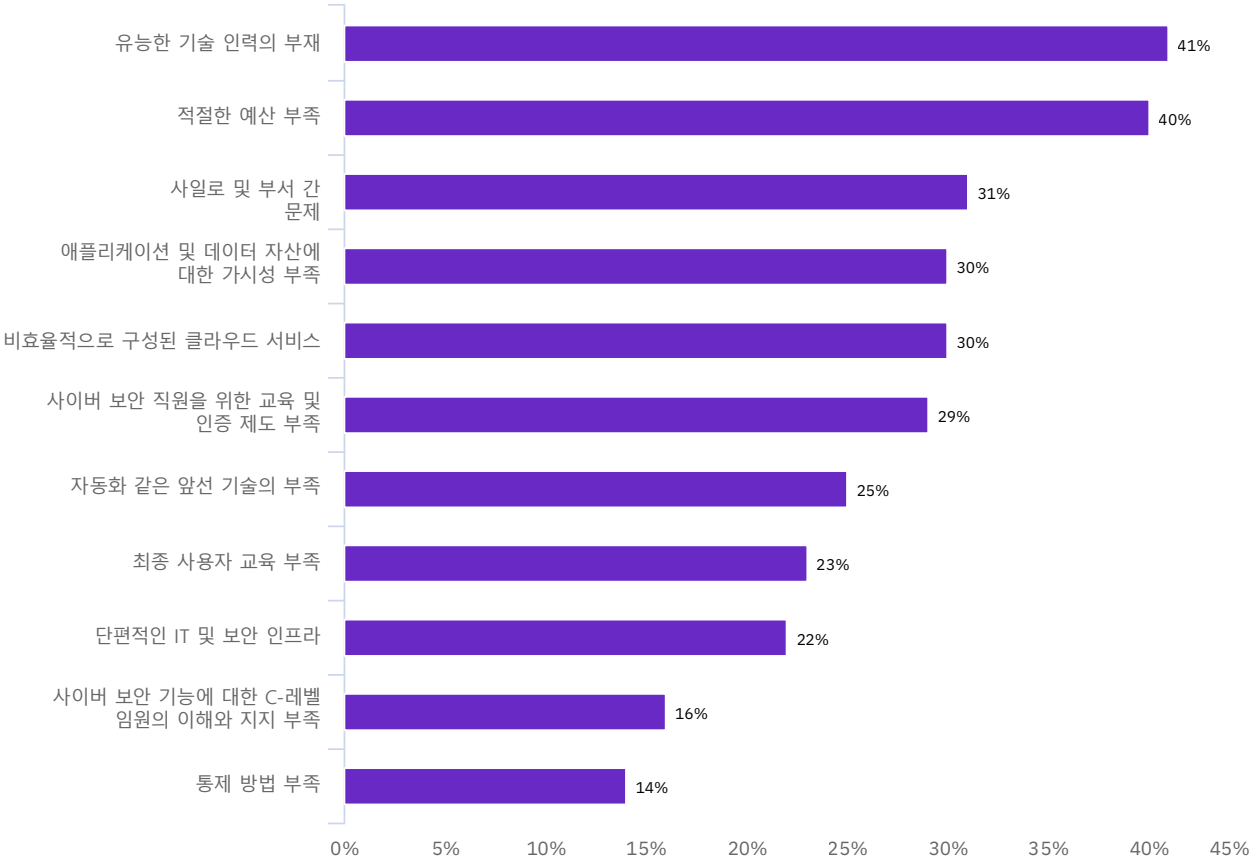


그림 4 는 조직이 자사 사이버 복원력이 향상되지 않았다고 생각하는 이유를 설명합니다. 사람과 프로세스, 기술을 조화롭게 활용하는 것이 도전 과제가 되었습니다.

그림 5

클라우드 서비스 사용이 사이버 복원력 개선을 가져온 요인

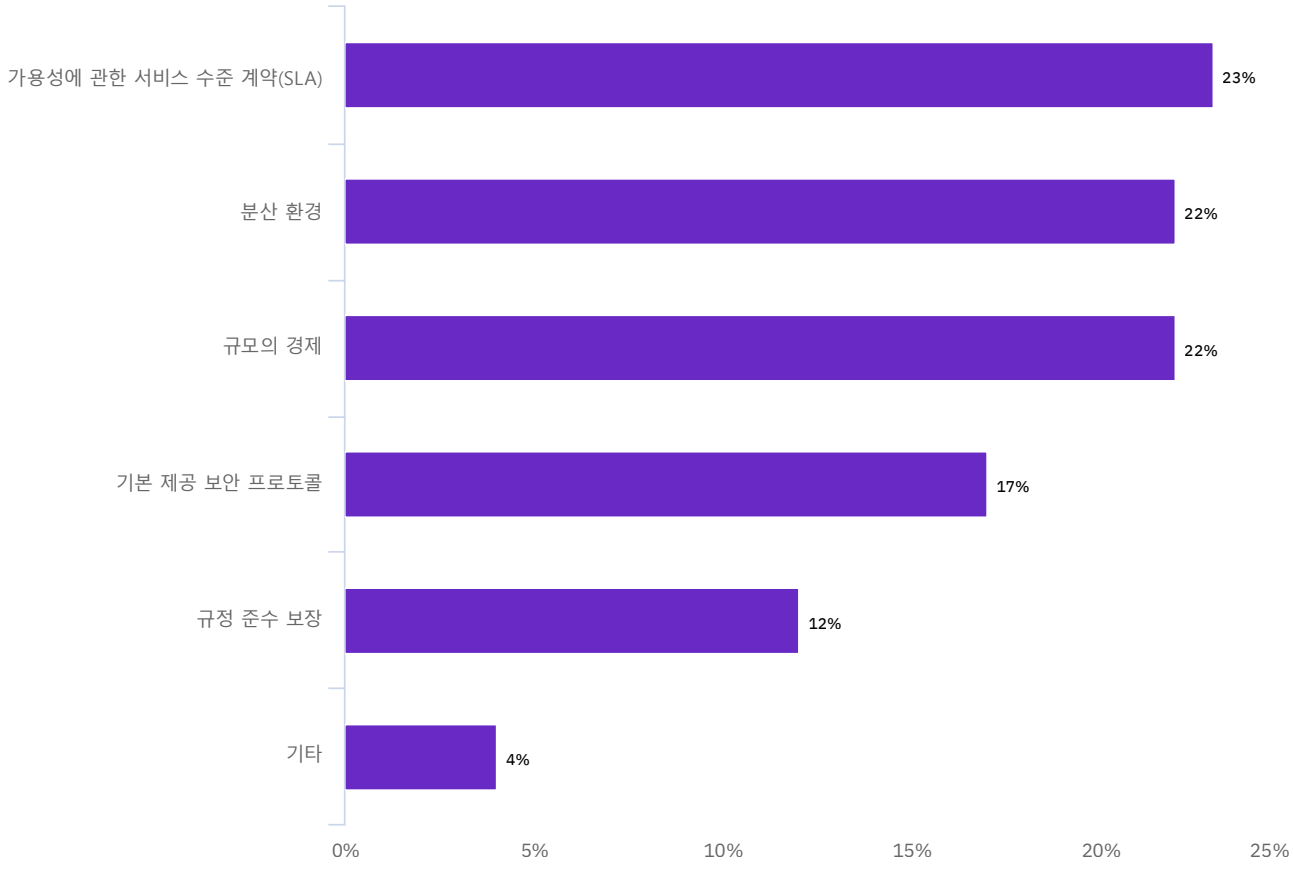


그림 5 는 클라우드 서비스 사용이 조직의 사이버 복원력 개선이 도움이 된 요인을 분석합니다. 상위 3개 요인은 가용성에 관한 서비스 수준 계약, 분산 환경 그리고 규모의 경제였습니다.

그림 6

사용된 공격 계획

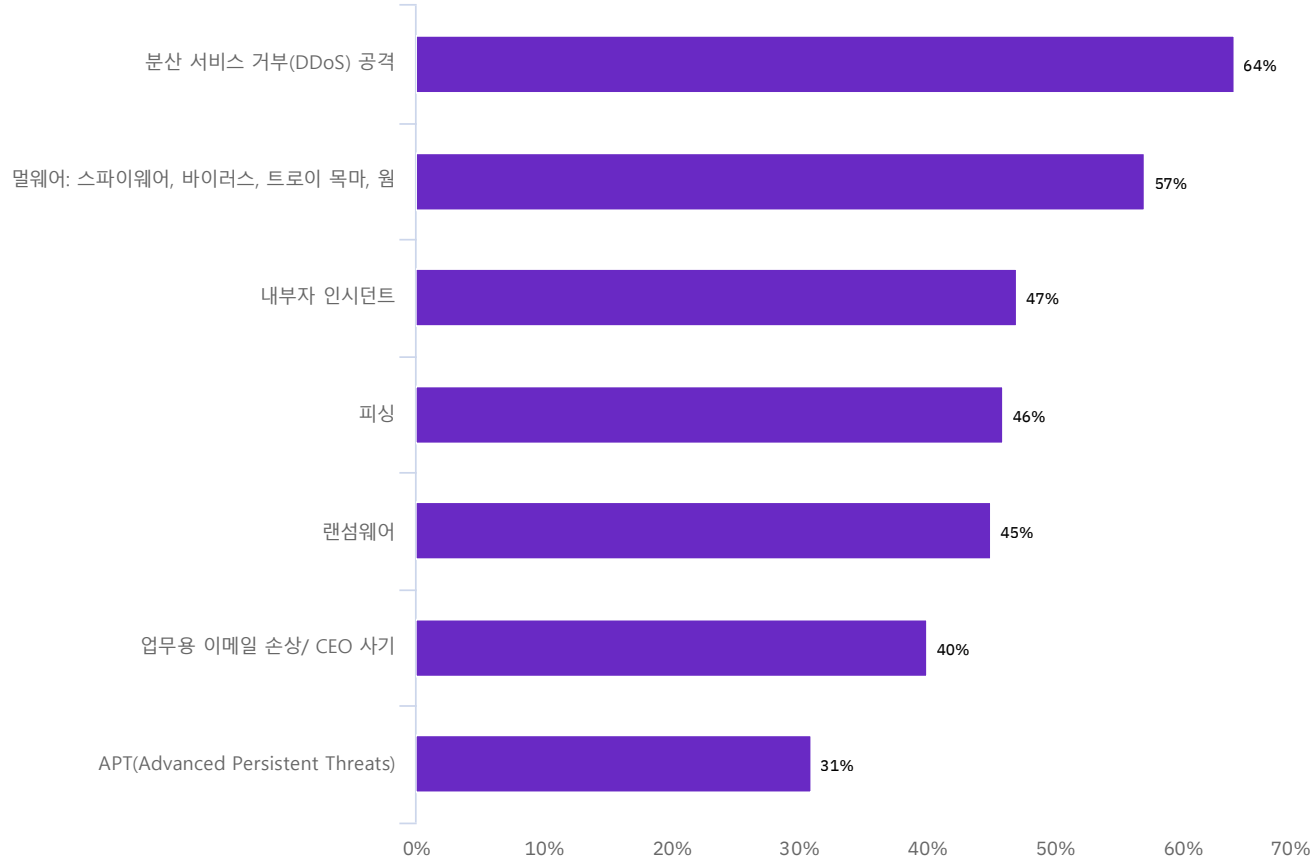


그림 6 은 조직이 수립한 유형별 대응 계획의 위협 유형을 세부적으로 보여줍니다. DDoS 공격과 멀웨어, 내부자 공격이 3대 유형입니다.

그림 7

심각도 측정 척도

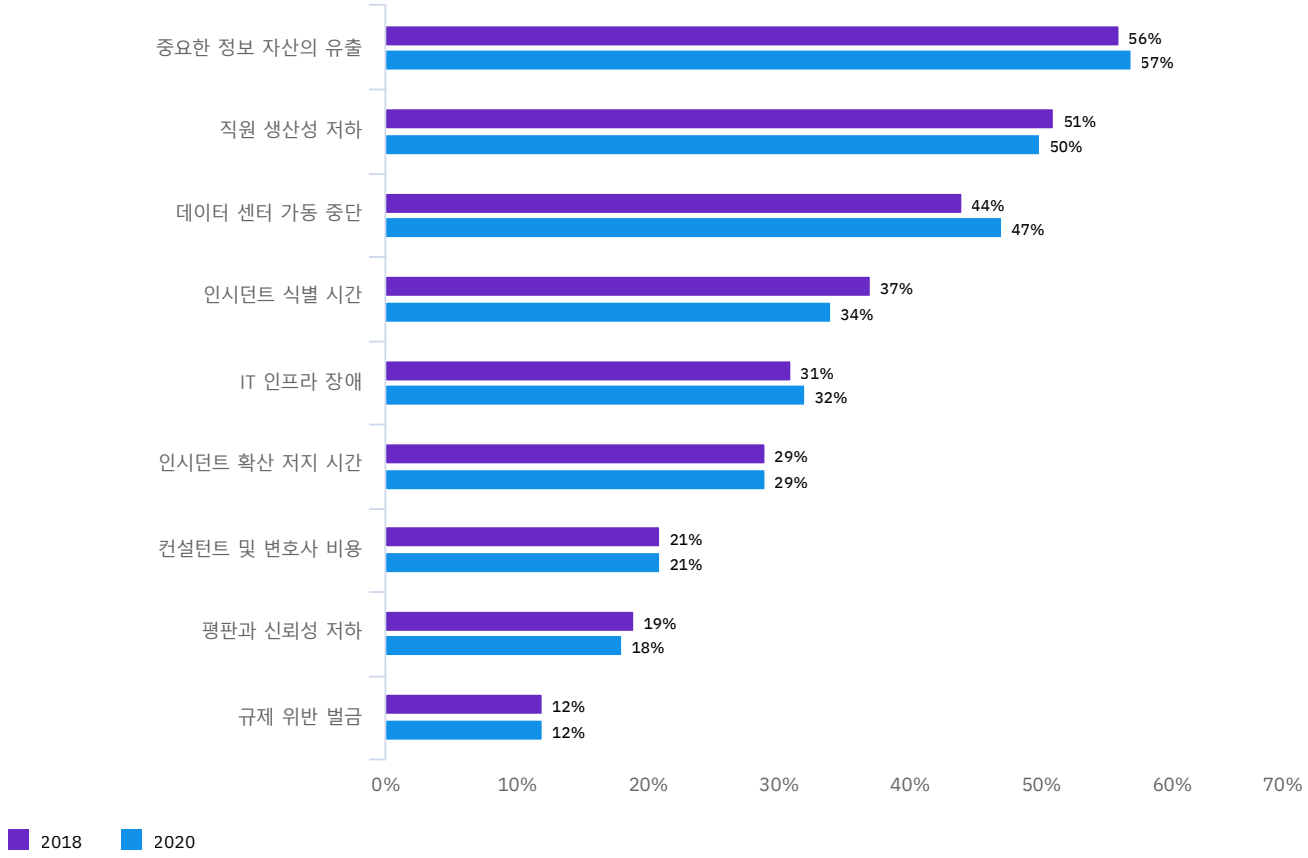


그림 7 은 지난 2년 동안 중요한 정보 자산의 유출이 가장 중요한 척도로 유지되는 가운데 조직이 공격의 심각도를 측정하는 척도를 보여줍니다.

그림 8

위협 인텔리전스가 사이버 복원력을 개선하는 방법

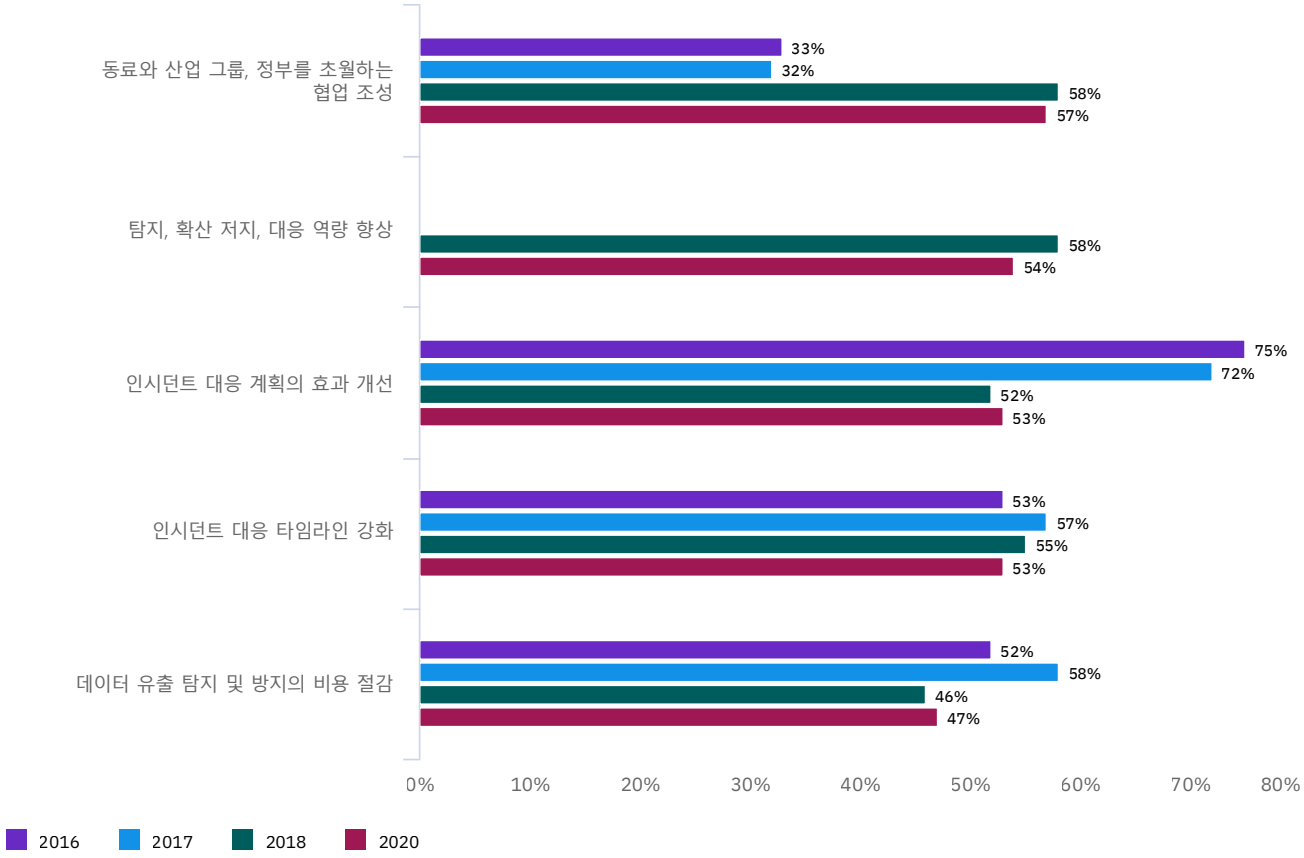


그림 8 위협 인텔리전스를 공유할 때 얻을 수 있는 가치를 평가합니다. 지난 4년 동안 자사 인시던트 대응 계획의 효과를 개선할 수 있다는 응답자들의 믿음이 29% 감소했습니다.

그림 9

우수 조직의 개선 원인

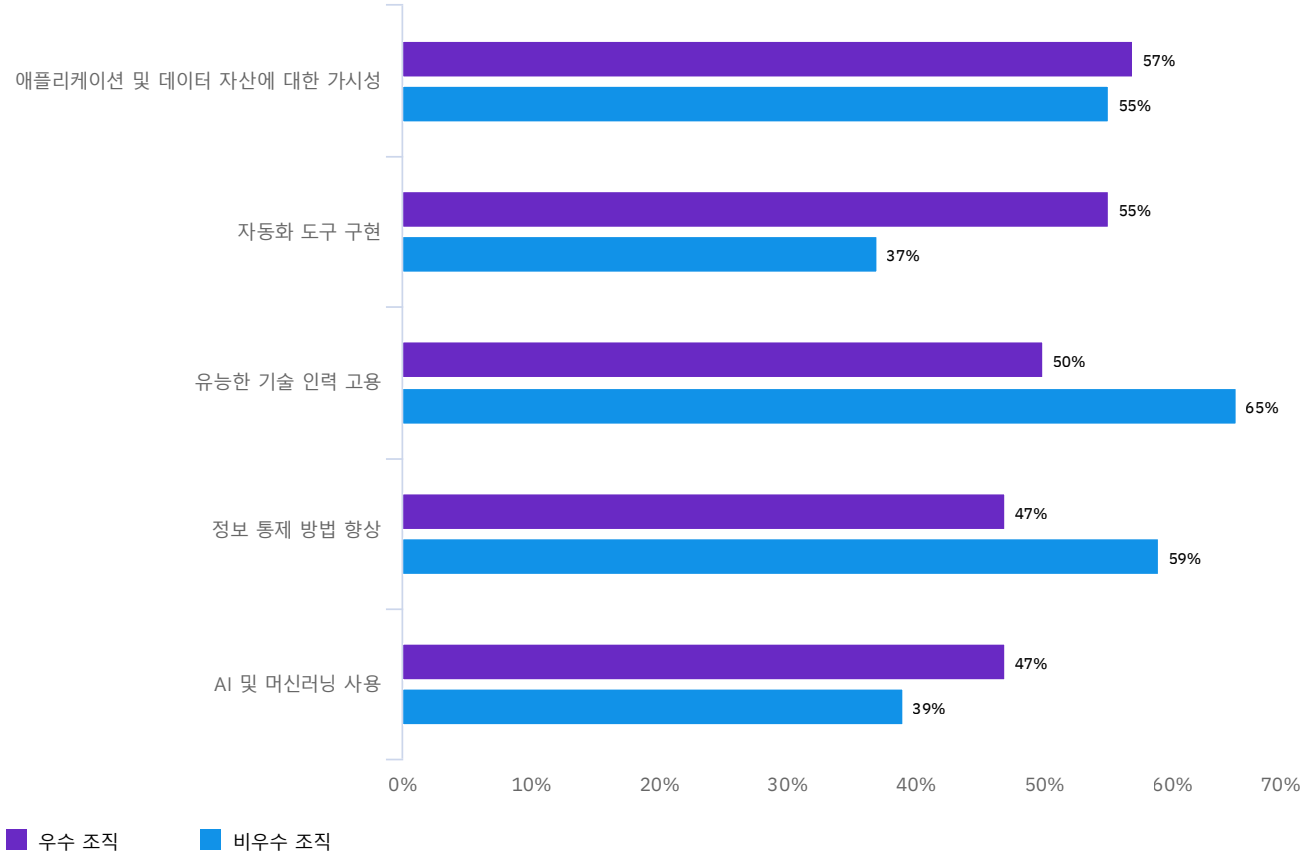


그림 9 는 비우수 조직에 비해 우수 조직의 사이버 복원력이 개선될 수 있었던 이유를 보여줍니다.

그림 10

우수 조직이 사이버 복원력이 뛰어난 기업으로 탈바꿈하는 이유

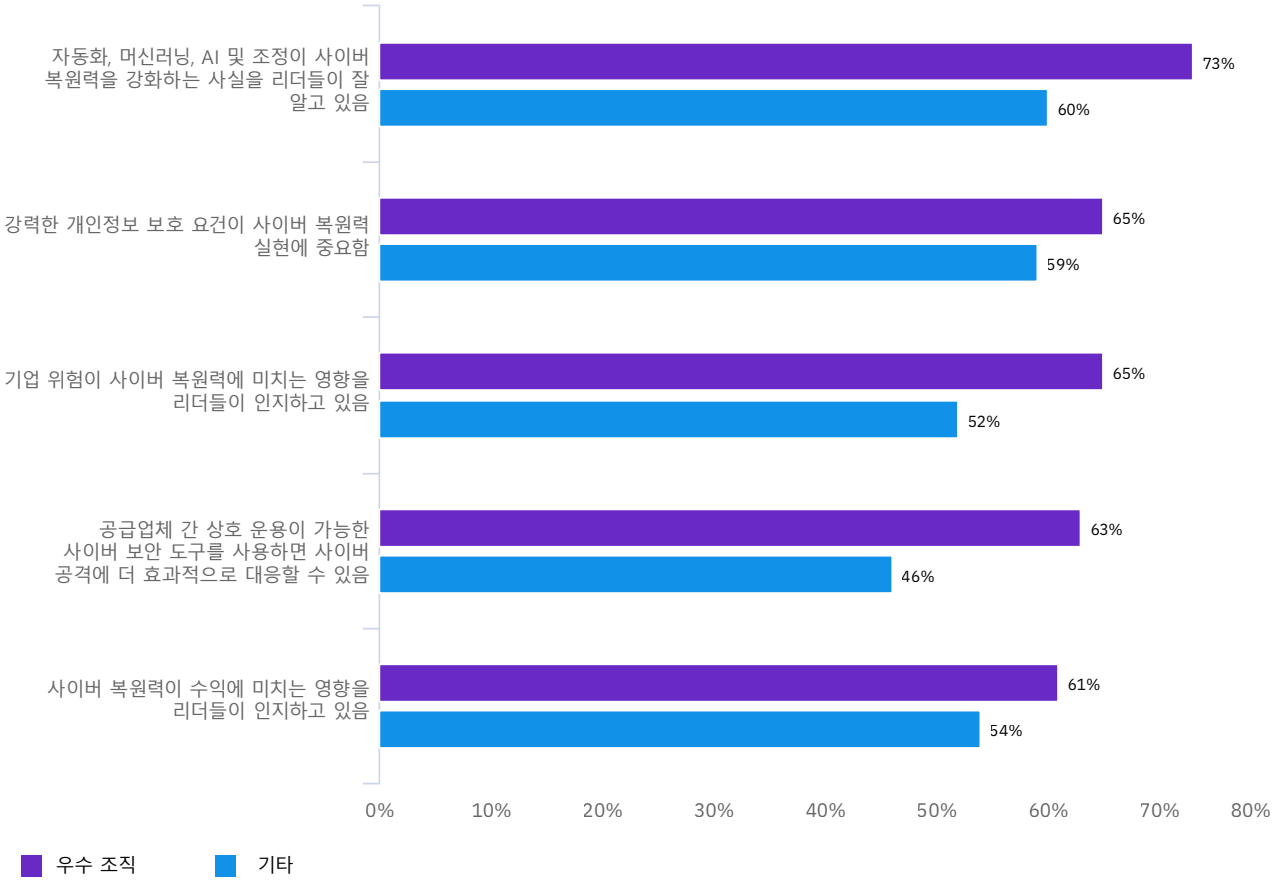


그림 10 은 우수 조직이 사이버 복원력이 뛰어난 기업으로 탈바꿈하는 이유를 보여줍니다.

그림 11

우수 조직의 사이버 복원력 신뢰도 수준

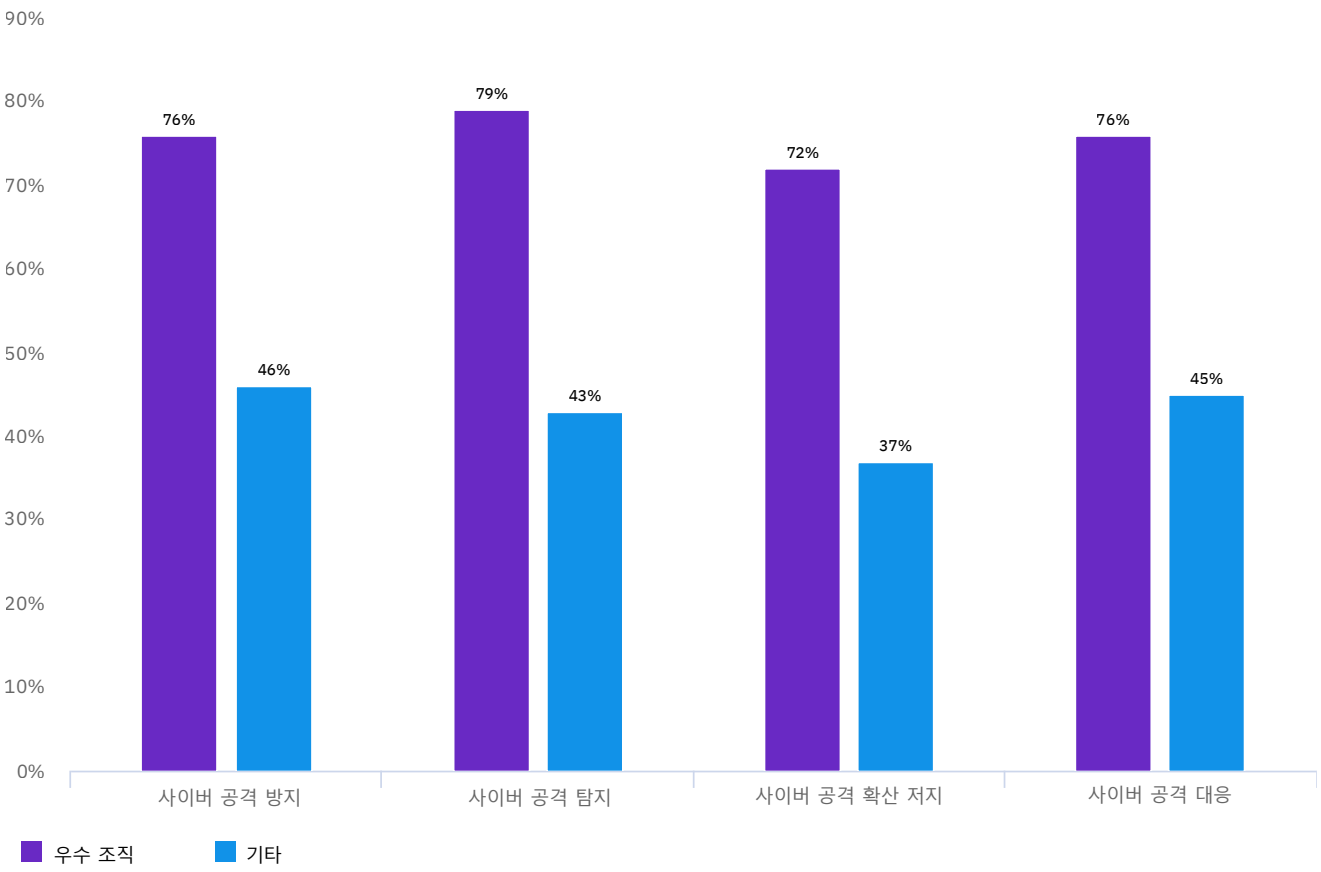


그림 11 은 우수 조직의 사이버 공격 관련 신뢰도를 보여줍니다. 우수 조직과 비우수 조직에서 차이가 가장 큰 부문은 사이버 공격 탐지 역량입니다.

그림 12

보안 솔루션의 수가 인시던트 대응에 미치는 영향

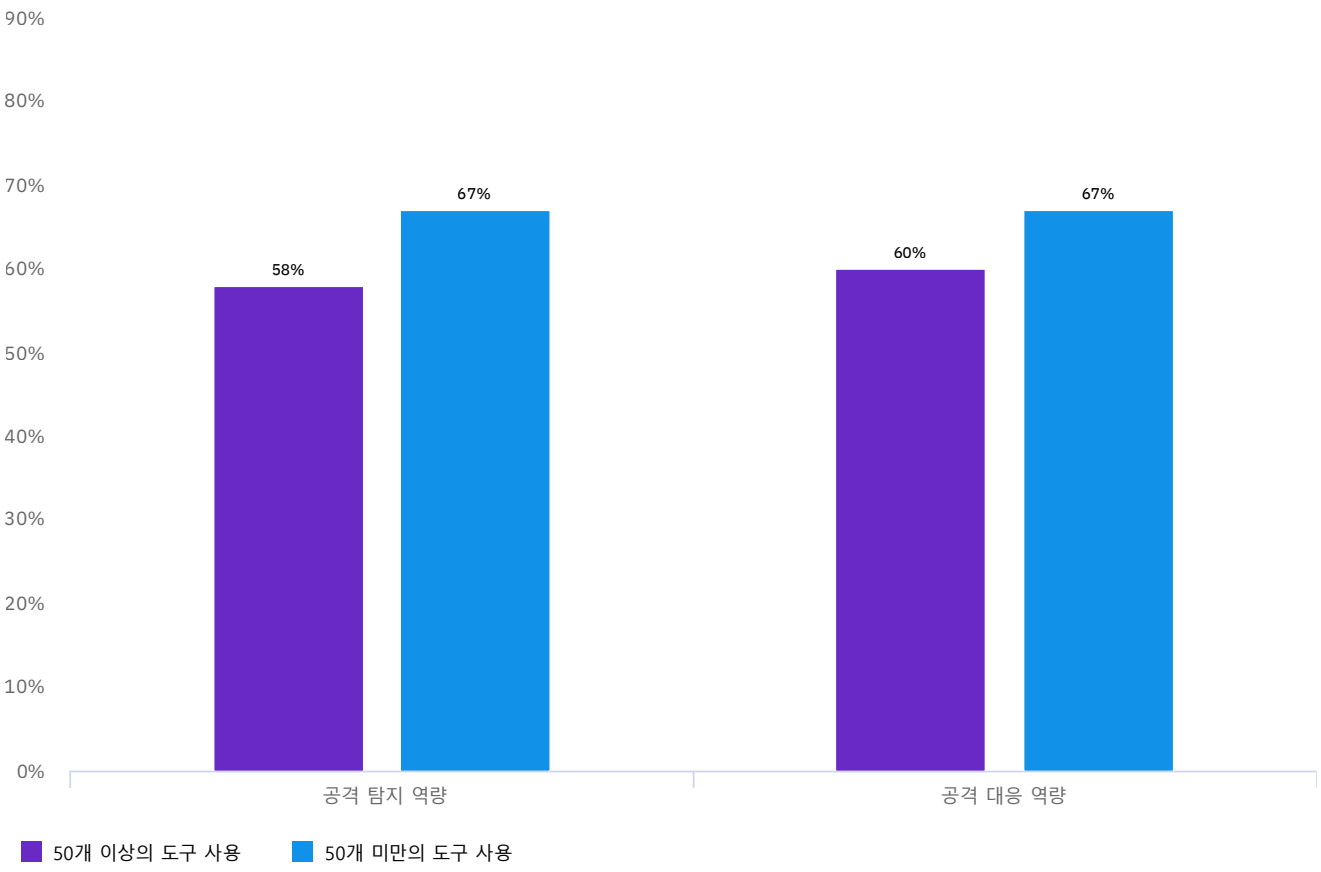


그림 12 는 50개 이상의 보안 솔루션을 사용할 때 인시던트 대응에 미치는 영향을 보여줍니다. 50개 미만의 도구를 사용한 조직이 더 우수한 사이버 공격 처리 역량을 보고했습니다.

그림 13

지역에 따른 공격별 대응 계획 사용

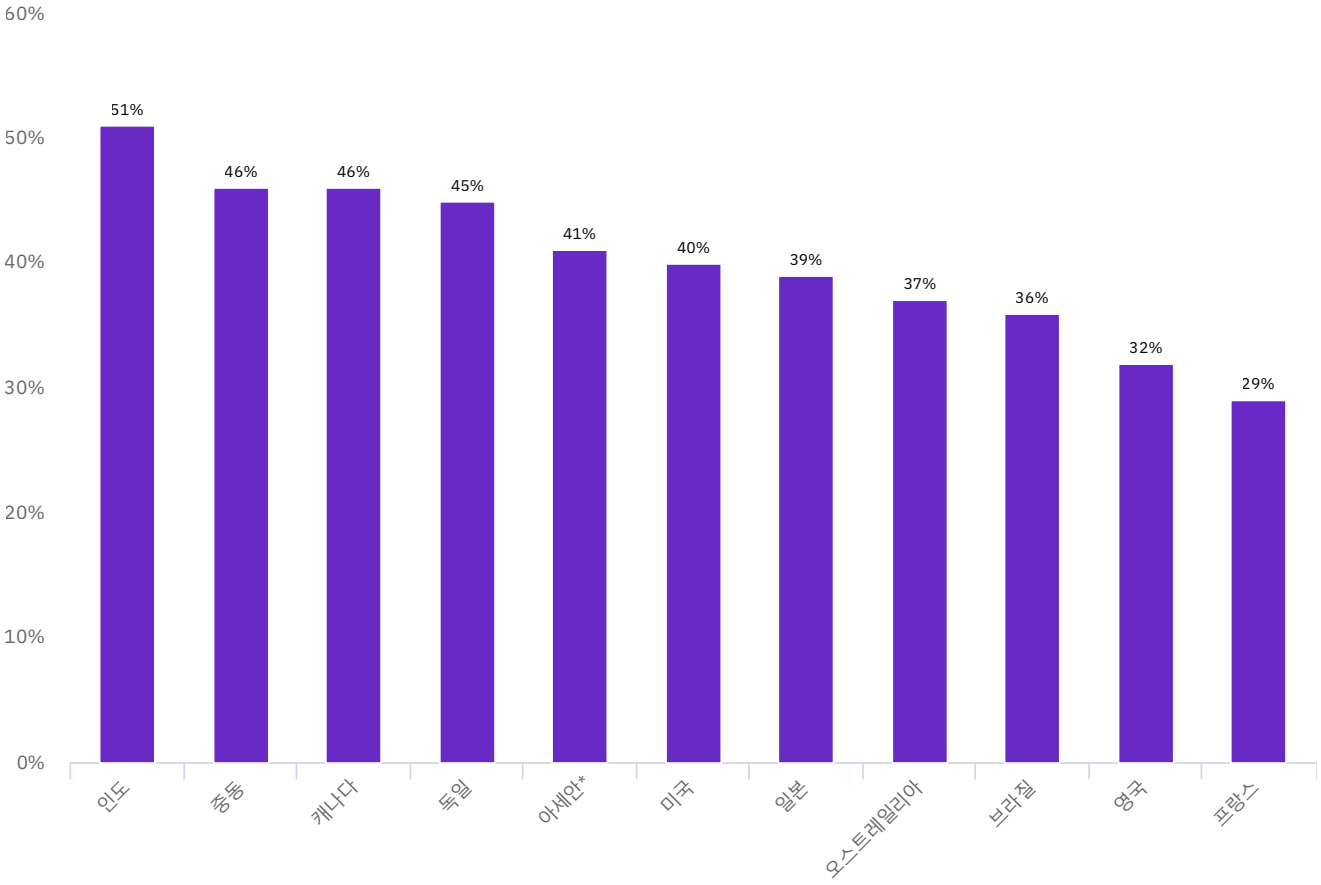


그림 13 은 조사에서 드러난 국가별 차이를 보여줍니다. 인도의 조직이 다양한 사이버 공격 유형별 대응 계획을 마련해 놓았을 가능성이 높고, 영국과 프랑스는 대응 계획을 마련해 놓았을 가능성이 가장 낮았습니다.

*아세안은 싱가포르, 필리핀, 베트남, 태국, 말레이시아, 인도네시아에 거주하는 응답자 표본을 나타냅니다.

**중동은 아랍에미리트 연합과 사우디아라비아에 거주하는 응답자 표본을 나타냅니다.

그림 14

우수한 사이버 복원력 실현에서 지역별 클라우드 서비스의 가치

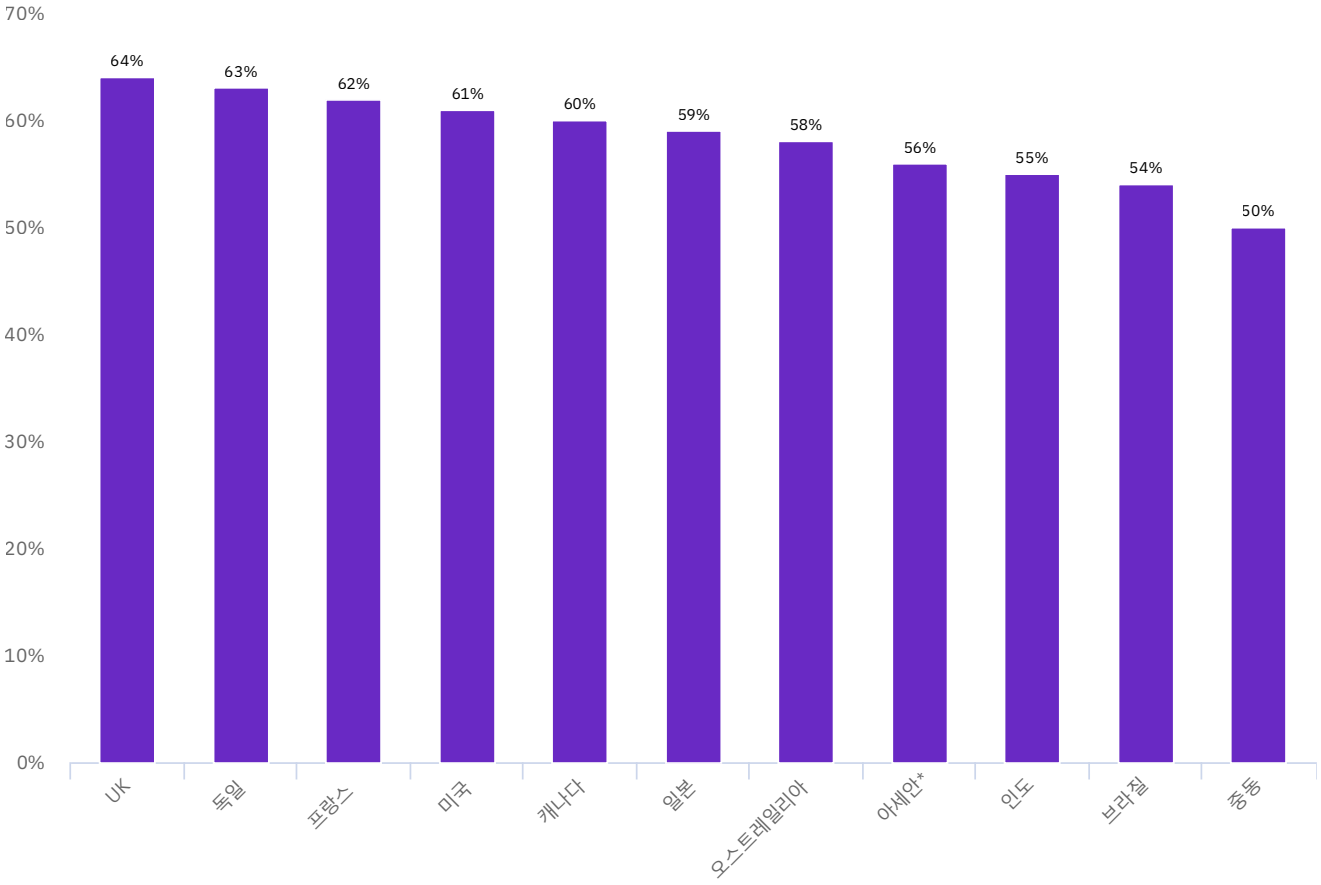


그림 14 는 클라우드 서비스가 사이버 복원력에 미치는 영향의 지역별 차이를 보여줍니다. 영국, 독일, 프랑스, 미국이 밀접하게 연결되어 있었습니다.

*아세안은 싱가포르, 필리핀, 베트남, 태국, 말레이시아, 인도네시아에 거주하는 응답자 표본을 나타냅니다.

**중동은 아랍에미리트 연합과 사우디아라비아에 거주하는 응답자 표본을 나타냅니다.

그림 15

업종별로 클라우드 서비스 사용이 사이버 복원력 개선에 미치는 영향*

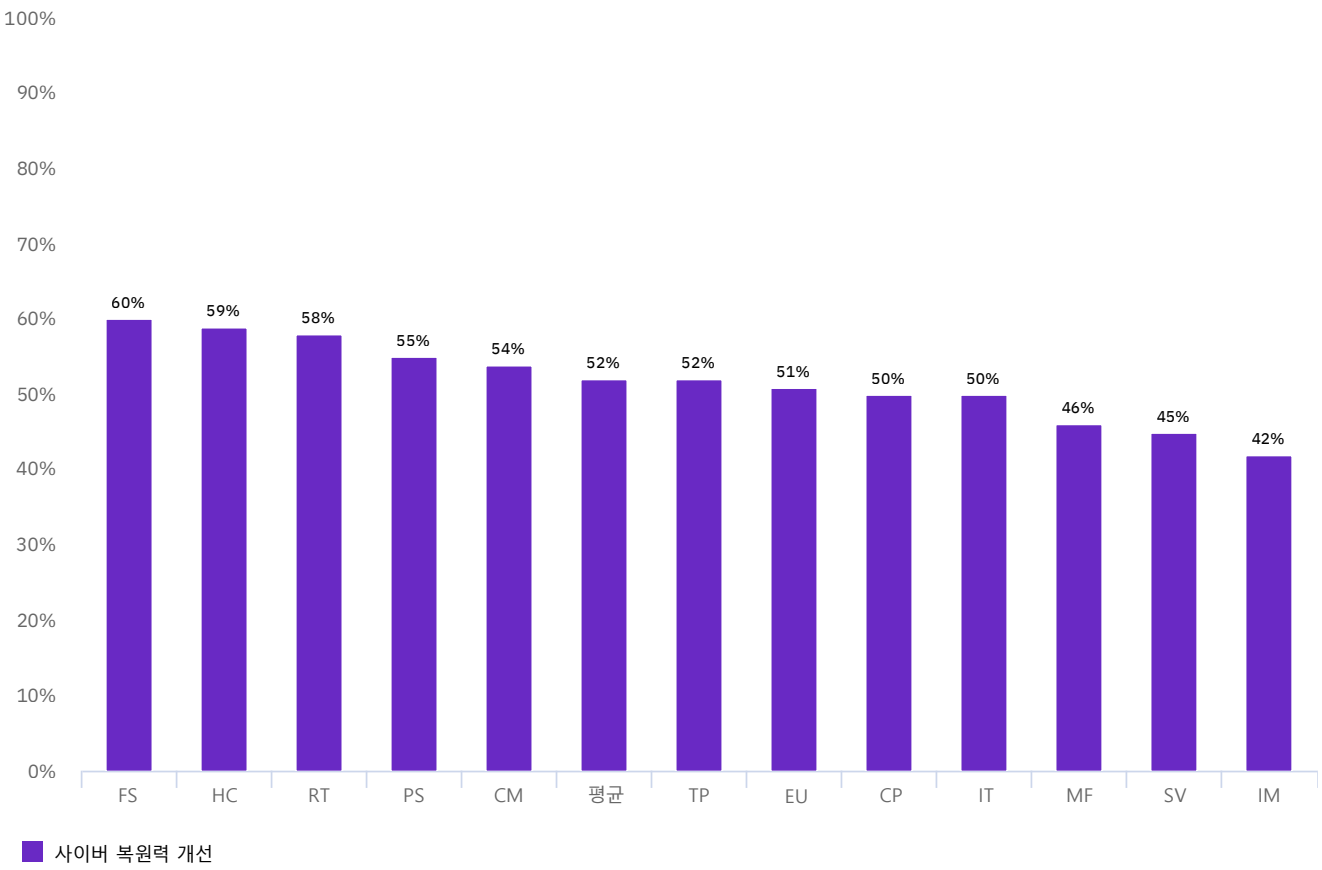


그림 15 는 클라우드 서비스 사용이 사이버 복원력 개선에 미치는 영향의 업종별 차이를 보여줍니다.

*업종 약어: 금융 서비스(FS), 의료 및 의약품(HC), 공공 부문(PS), 소매(RT), 서비스(SV), 산업(IM), 에너지 및 유틸리티(EU), IT 및 기술(IT), 제조(MF), 소비재(CP), 통신(CM), 운송(TP), 엔터테인먼트 및 미디어(EM), 교육 및 연구(ED), 호텔경영(HP), 방위 및 항공우주(DF), 농업 및 식품 서비스(AG), 물류 및 유통(LD). 업종 정의의 전체 목록은 34페이지를 참조하십시오.

그림 16

업종별 CSIRP 사용 방식의 차이*

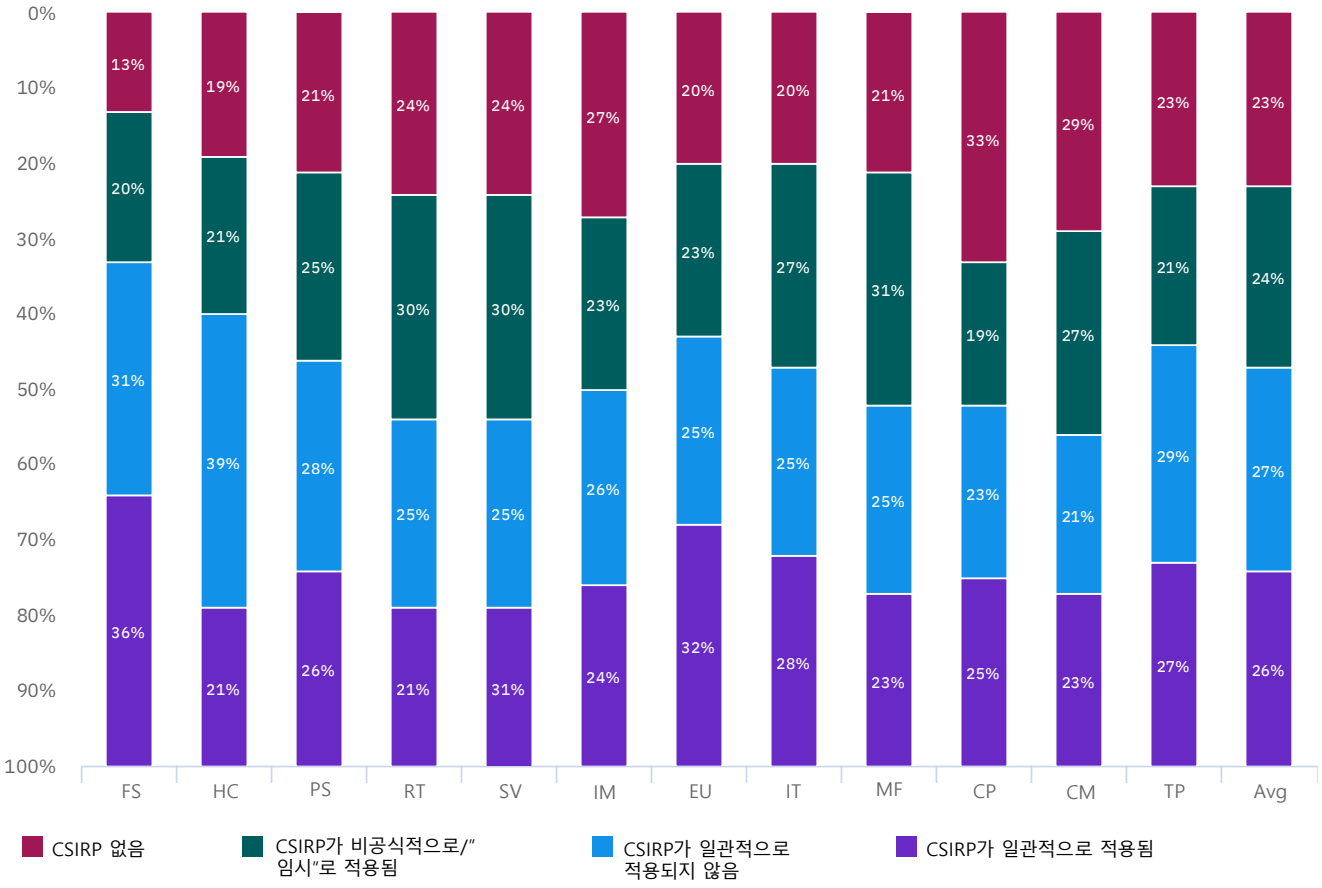


그림 16 은 CSIRP 사용의 업종별 차이를 보여줍니다.

*업종 약어: 금융 서비스(FS), 의료 및 의약품(HC), 공공 부문(PS), 소매(RT), 서비스(SV), 산업(IM), 에너지 및 유틸리티(EU), IT 및 기술(IT), 제조(MF), 소비재(CP), 통신(CM), 운송(TP), 엔터테인먼트 및 미디어(EM), 교육 및 연구(ED), 호텔경영(HP), 방위 및 항공우주(DF), 농업 및 식품 서비스(AG), 물류 및 유통(LD). 업종 정의의 전체 목록은 34페이지를 참조하십시오.

그림 17

사이버 보안의 투자를 정당화하는 요인

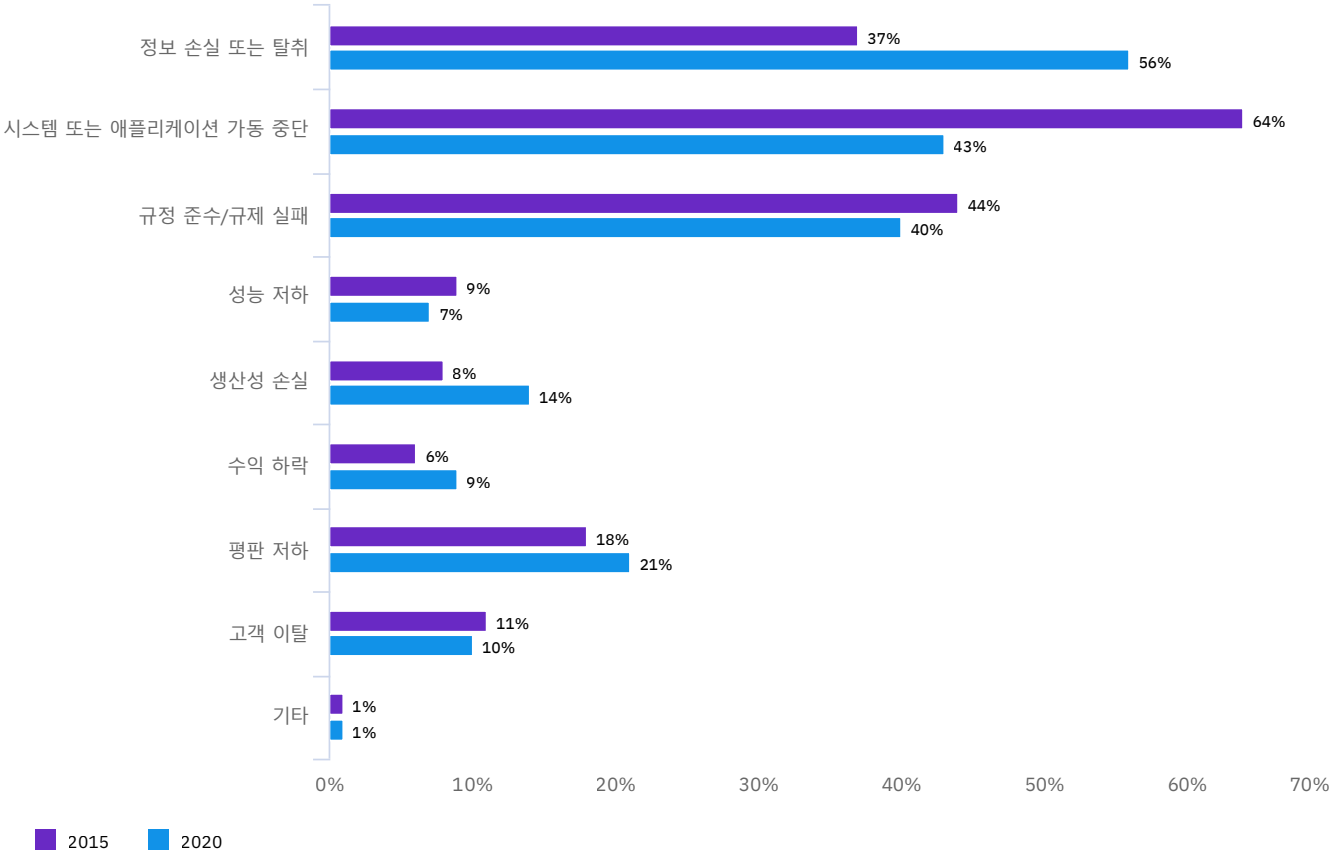


그림 17 은 사이버 보안 투자를 정당화하는 요인을 보여줍니다. 2015년 이후 예산 정당성의 근거가 시스템 또는 애플리케이션 가동 중단에서 정보 손실 또는 탈취로 변경되었습니다.

그림 18

사이버 복원력에 할당되는 사이버 보안 예산

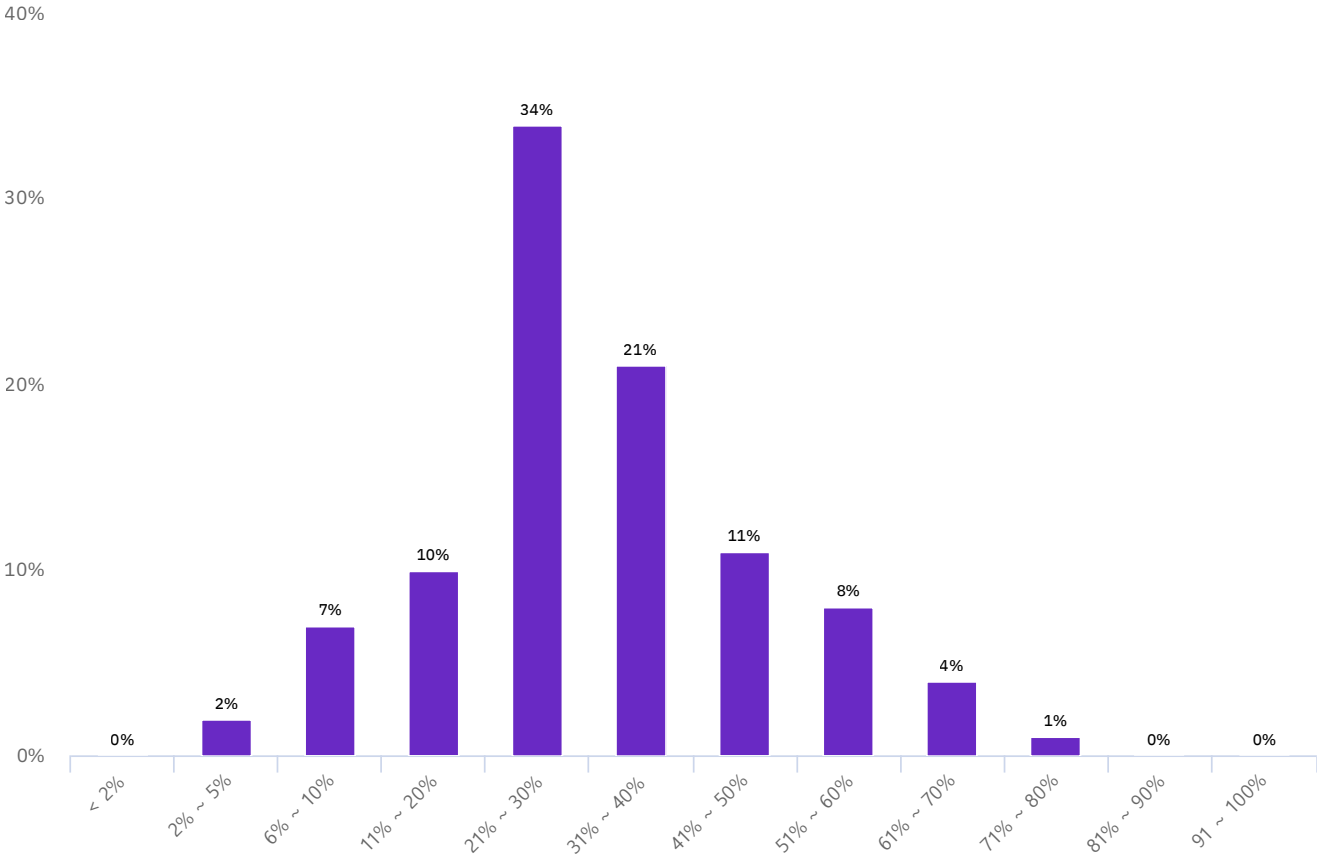


그림 18 은 사이버 복원력 관련 활동에 할당되는 예산의 비율을 보여줍니다.

참여 조직 특징

본 2020년 사이버 복원력 우수 조직 보고서에는 미국, 인도, 독일, 영국, 브라질, 일본, 호주, 프랑스, 캐나다, 아세안* 및 중동* 지역에서 설문조사에 참여한 3,439명 IT 및 보안 실무자들의 답변 내용이 분석되어 있습니다.

대표 업종

18개 업종이 표본에 포함되었습니다.

금융 서비스
은행, 보험, 투자 회사

의료 및 의약품
병원, 의원, 생의학 및 생명 과학

유통
재래식 소매 및 전자상거래

제조
대형 상품 또는 부품 생산업체

숙박
호텔, 레스토랑 체인, 유람선

공공 부문
연방, 주, 지방 정부 기관 및 NGO

운송
항공사 및 철도

에너지 및 유틸리티
오일 및 가스 회사, 유틸리티, 대체 에너지 생산업체 및 공급업체

소비재
소비재 제조업체 및 유통업체

물류 및 유통
트럭 및 운송 회사, 공급망 관리

산업
화학 처리, 엔지니어링 및 제조 회사

통신
신문, 서적 출판사, 광고 홍보 대행사

IT 및 기술
소프트웨어 및 하드웨어 회사

서비스
법률, 회계, 컨설팅 회사 같은 전문 서비스

엔터테인먼트 및 미디어
영화 제작, 스포츠, 게임 및 카지노

농업 및 식품 서비스
농장, 상용 식품 생산업체(식물 및 가축)

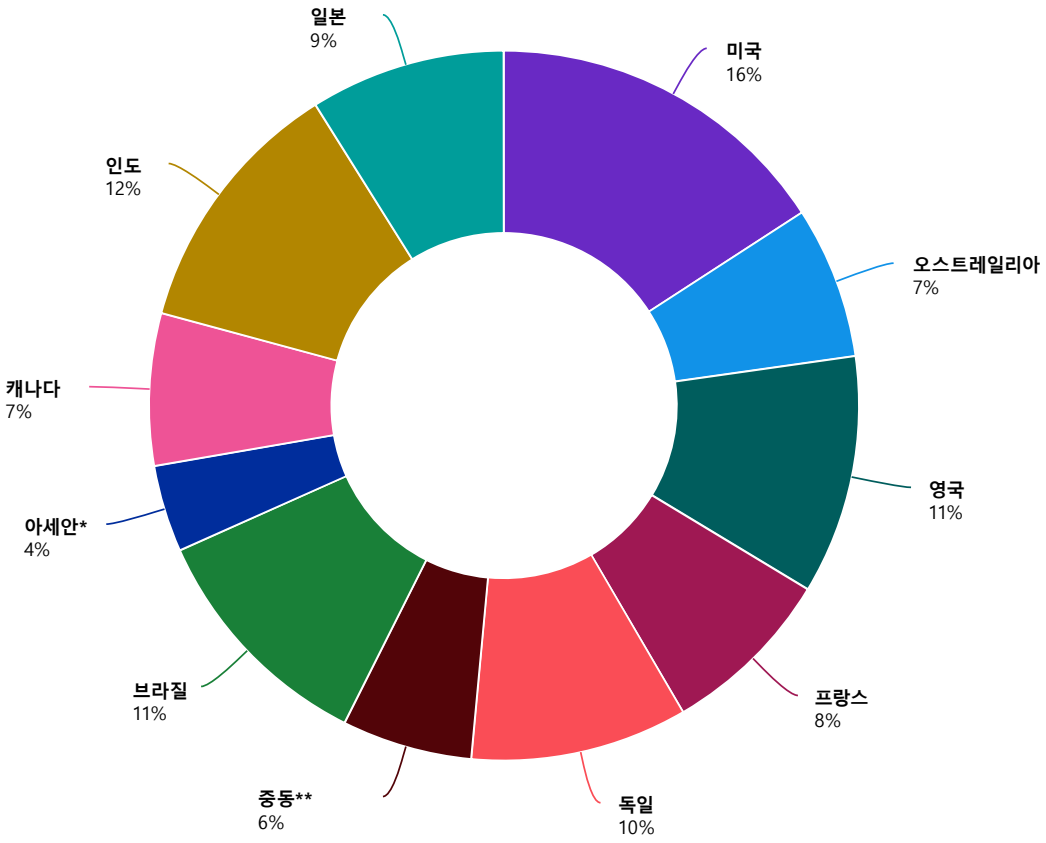
방위 및 항공우주
상용 또는 방위 관련 항공기 및 시스템의 생산업체와 설계업체

교육 및 연구
시장 연구, 싱크탱크, R&D, 공립 및 사립 대학/전문대학, 교육 개발 회사

*아세안은 싱가포르, 필리핀, 베트남, 태국, 말레이시아, 인도네시아에 거주하는 응답자 표본을 나타냅니다.
**중동은 아랍에미리트 연합과 사우디아라비아에 거주하는 응답자 표본을 나타냅니다.

그림 19

국가 또는 지역별 표본 분포



*아세안은 싱가포르, 필리핀, 베트남, 태국, 말레이시아, 인도네시아에 거주하는 응답자 표본을 나타냅니다.

**중동은 아랍에미리트 연합과 사우디아라비아에 거주하는 응답자 표본을 나타냅니다.

그림 20

업종별 표본 분포

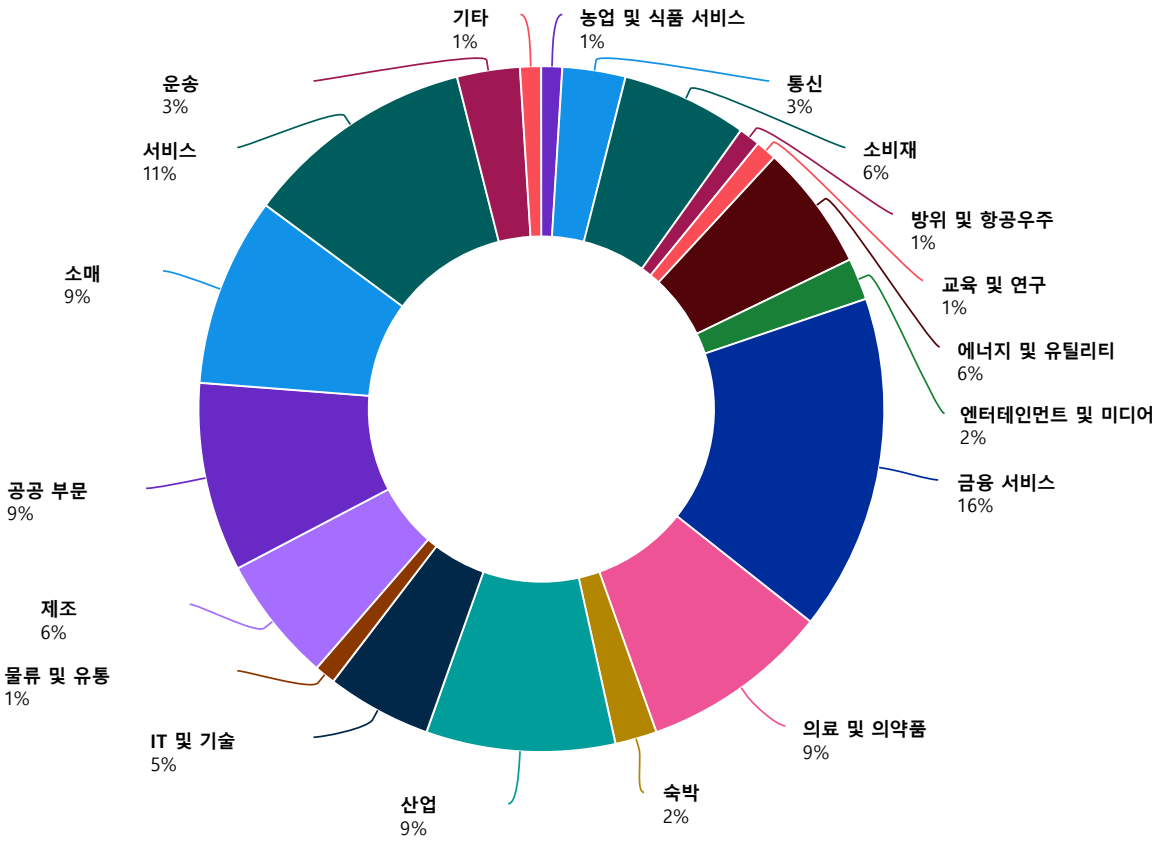


그림 21
직무별 분포

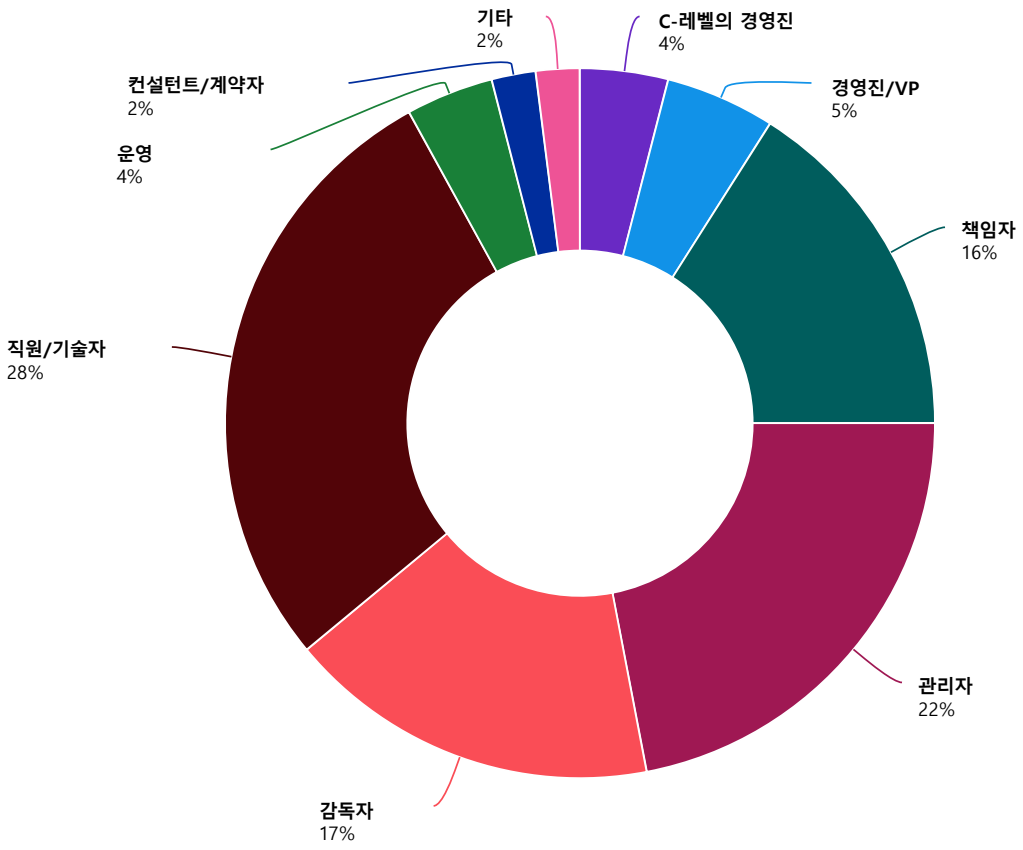
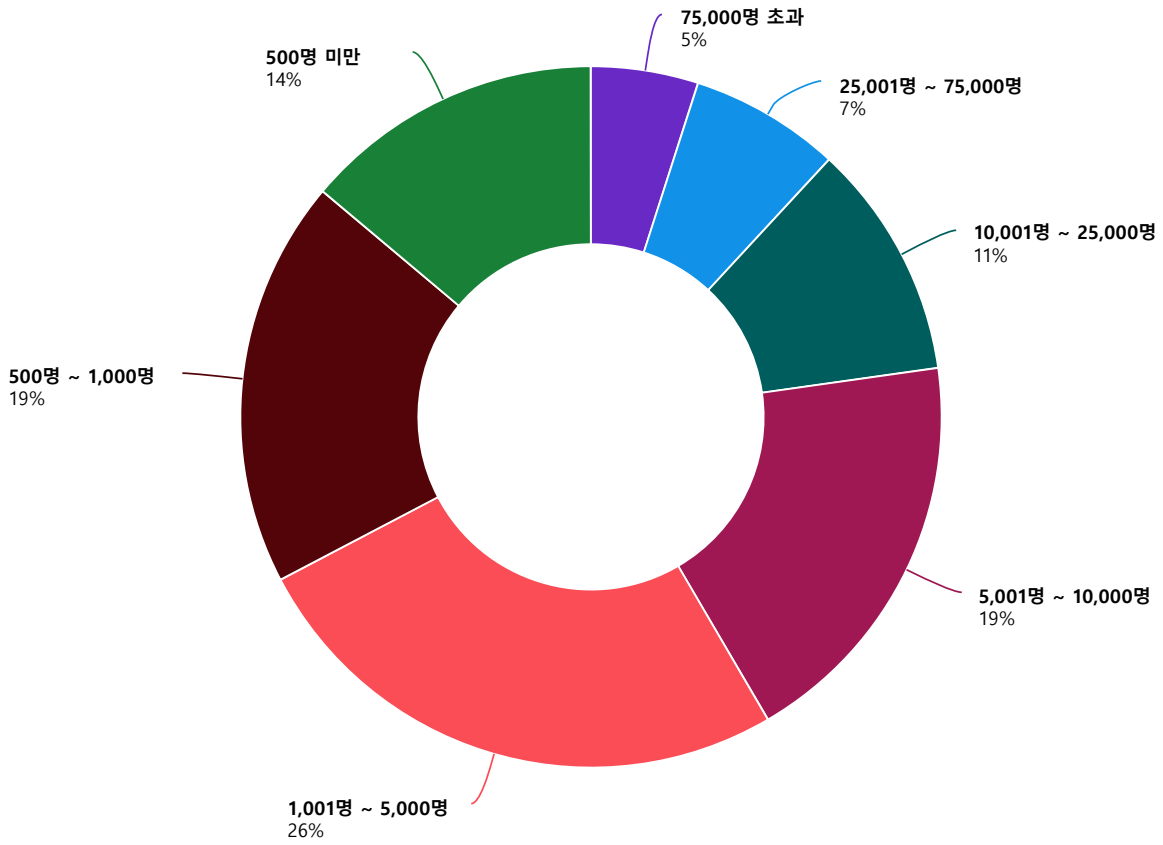

기타
2%
C-레벨의 경영진
4%
경영진/VP
5%
컨설턴트/계약자
2%
운영
4%
책임자
16%
직원/기술자
28%
관리자
22%
감독자
17%

그림 22

회사 크기별 분포



방법

미국, 인도, 독일, 영국, 브라질, 일본, 호주, 프랑스, 캐나다, 아세안 및 중동 지역의 IT 및 보안 실무자들을 대상으로 온라인 설문조사를 실시했습니다.

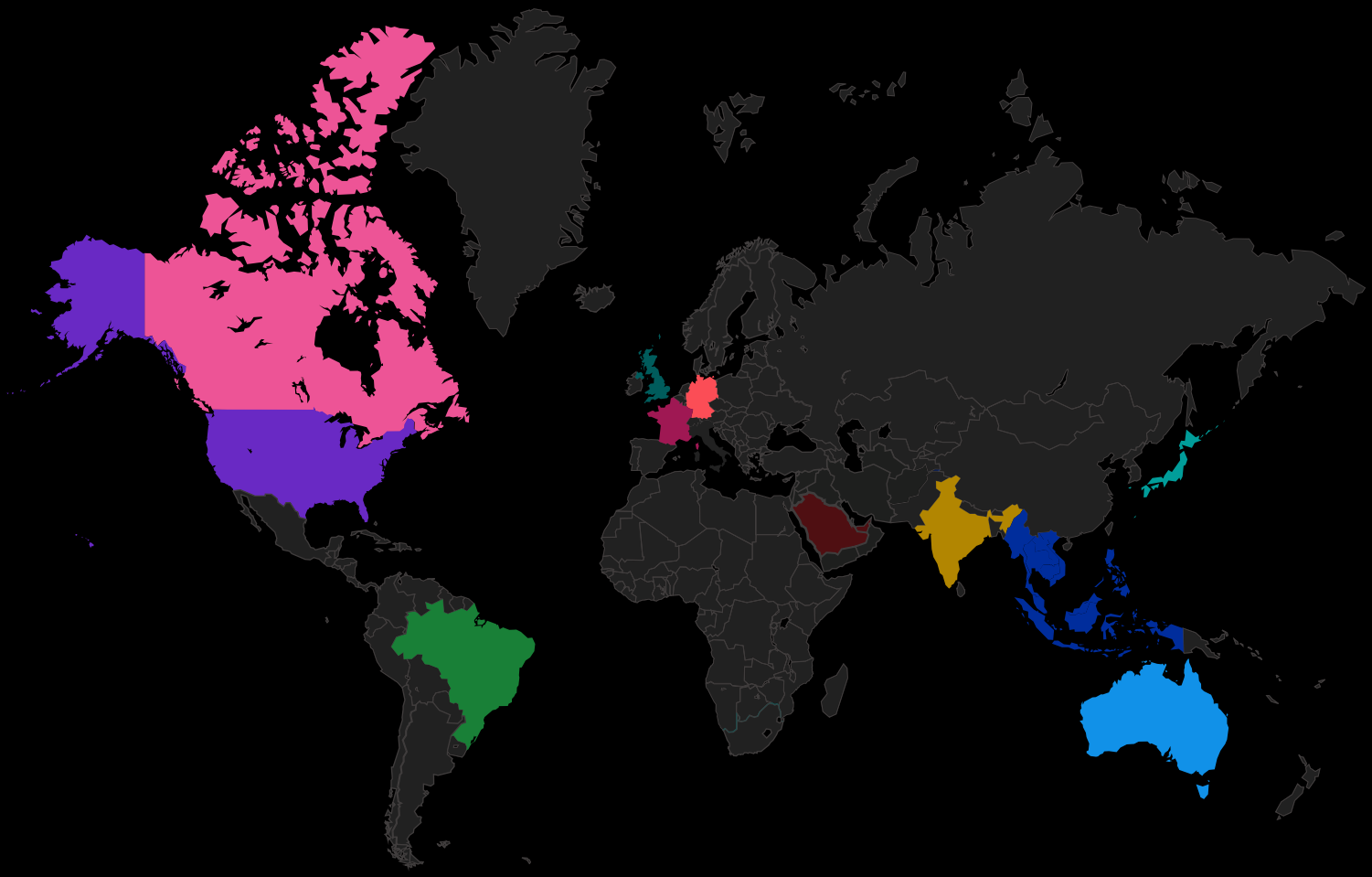
설문조사 응답자의 최종 표본은 3,439명이고, 전체 응답률은 3.3%입니다.

11

국가 및 지역

3,439

응답자



*아세안은 싱가포르, 필리핀, 베트남, 태국, 말레이시아, 인도네시아에 거주하는 응답자 표본을 나타냅니다.

**중동은 아랍에미리트 연합과 사우디아라비아에 거주하는 응답자 표본을 나타냅니다.

정의

사이버 복원력

사이버 복원력은 사이버 공격을 관리, 완화하고 극복하는 데 필요한 방지, 탐지, 대응 역량을 총체적으로 정의하는 용어입니다. 사이버 공격 발생 시 핵심 목표와 무결성을 유지하는 기업의 역량을 나타냅니다. 사이버 복원력 우수 기업은 데이터와 애플리케이션, IT 인프라를 공격하는 다양한 위협을 방지, 탐지, 확산 저지하고 복구할 수 있는 조직을 의미합니다.

우수 조직

이번 조사의 일환으로 사이버 복원력의 수준을 높여 위험과 취약점, 공격을 효과적으로 완화할 수 있게 되었다고 스스로 평가한 응답자를 가려냈습니다. IBM은 이러한 조직을 사이버 복원력 우수 조직이라고 부릅니다.

조사 제한사항

설문조사는 기본적으로 결과에서 어떤 사실을 추론하기 전에 주의 깊게 고려해야 하는 제한 사항이 있습니다. 대부분의 웹 기반 설문조사가 갖는 제한사항은 다음과 같습니다.

무응답 편향

현재 결과는 설문조사에 응답한 표본을 바탕으로 합니다. 당사는 조직을 대표할 수 있는 개인 표본에게 설문조사를 발송했기 때문에 반환된 유효 응답의 수가 많았습니다. 무응답 테스트에도 불구하고 항상 설문조사에 참여하지 않은 개인과 설문조사를 완료한 개인의 기본 생각에는 상당한 차이가 있을 수 있습니다.

표본 추출 프레임 편향

정확성은 접촉 정보와 설문조사에 참여한 IT 또는 IT 보안 실무자 개인이 갖는 대표성의 정도에 따라 결정됩니다. 또한 미디어 보도와 같은 외부 이벤트에 따라 결과가 편향될 수 있음을 인정합니다. 마지막으로, 웹 기반 수집 방법을 사용했기 때문에 웹이 아닌 메일이나 전화 통화로 설문조사 답변을 받았다면 결과 패턴이 달라질 수 있습니다.

자기 보고 결과

설문조사의 품질은 설문조사 참여자로부터 비밀 유지 조건으로 받은 답변의 진정성을 바탕으로 합니다. 점검하고 균형을 유지하기 위한 조치를 설문조사 절차에 적용할 수 있으며, 설문조사 참여자가 정확한 답변을 제공하지 않을 가능성은 항상 존재합니다.

Ponemon Institute 및 IBM Security 정보

사이버 복원력 우수 조직 보고서 는 Ponemon Institute와 IBM Security가 공동으로 제작하였습니다. Ponemon Institute에서 독립적으로 설문조사를 실시하고 IBM Security에서 후원 및 분석하여 결과를 도출하고 보고서를 발행했습니다.

보고서 인용 또는 복제 허가를 받고 싶거나 본 조사 보고서에 대해 궁금한 점이나 의견이 있으시면 우편, 전화 또는 이메일로 문의해 주시기 바랍니다.

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

1.800.887.3118
research@ponemon.org

Ponemon Institute

Ponemon Institute는 기업과 정부의 정보 및 개인정보 보호 관리 관행을 혁신하여 정보 관리에 책임을 다하는 문화를 구축하기 위해 노력하는 독립적 연구 및 교육 기관입니다. 사람 및 조직 관련 민감한 정보의 관리 및 보안에 영향을 미치는 중요 문제를 경험적으로 조사하고 유용한 결과를 도출하는 것을 사명으로 하고 있습니다.

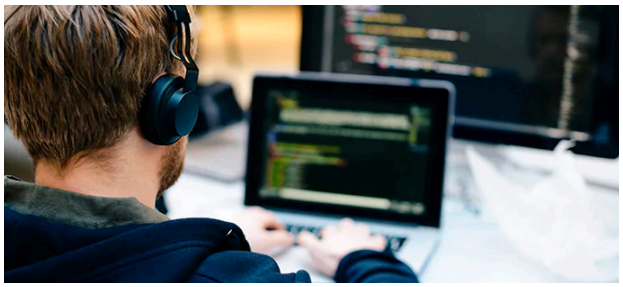
Ponemon Institute는 엄격한 데이터 비밀 유지, 개인정보 보호 및 윤리적 조사 표준을 준수하고, 개인 식별 정보(또는 기업 조사의 경우 회사 식별 정보)를 수집하지 않습니다. 뿐만 아니라 엄격한 품질 표준에 따라 설문조사 참여자에게 부적절하고 관련 없는 질문을 묻지 않습니다.

IBM Security

IBM Security는 기업 보안 제품 및 서비스를 위한 가장 앞선 통합형 포트폴리오 중 하나를 제공합니다. 세계적으로 유명한 IBM X-Force® 연구소가 지원하는 이 포트폴리오는 비즈니스 환경에 보안을 구축을 구축하여 불확실성의 시대에 성장할 수 있도록 돕는 보안 솔루션을 제공합니다.

IBM은 가장 광범위하고 깊이 있게 보안을 연구, 개발하고 제공하는 기업 중 하나입니다. 130여개국에서 매월 2조 개 이상의 이벤트를 모니터링하는 IBM은 3,000가지가 넘는 보안 특허를 보유하고 있습니다. 자세히 알아보려면 다음을 참조하세요.ibm.com/security.

다음 단계



멀티클라우드 환경에서 도구 통합

자세히 알아보기 →

위협 탐지

자세히 알아보기 →

대응 조정

자세히 알아보기 →

해결 및 복구

자세히 알아보기 →

한국아이비엠주식회사
(150-945) 서울시 영등포구 국제금융로 10
서울국제금융센터(Three IFC)

IBM 홈 페이지:
ibm.com

IBM **Security**