CISCO
SECURE

The bridge to possible

중소기업을 위한 사이버 보안: 아시아 태평양 지역 기업의 디지털 방어 대비

2021년 9월

목차

서문

새로운 디지털 노멀의 기반이 되는 사이버 보안

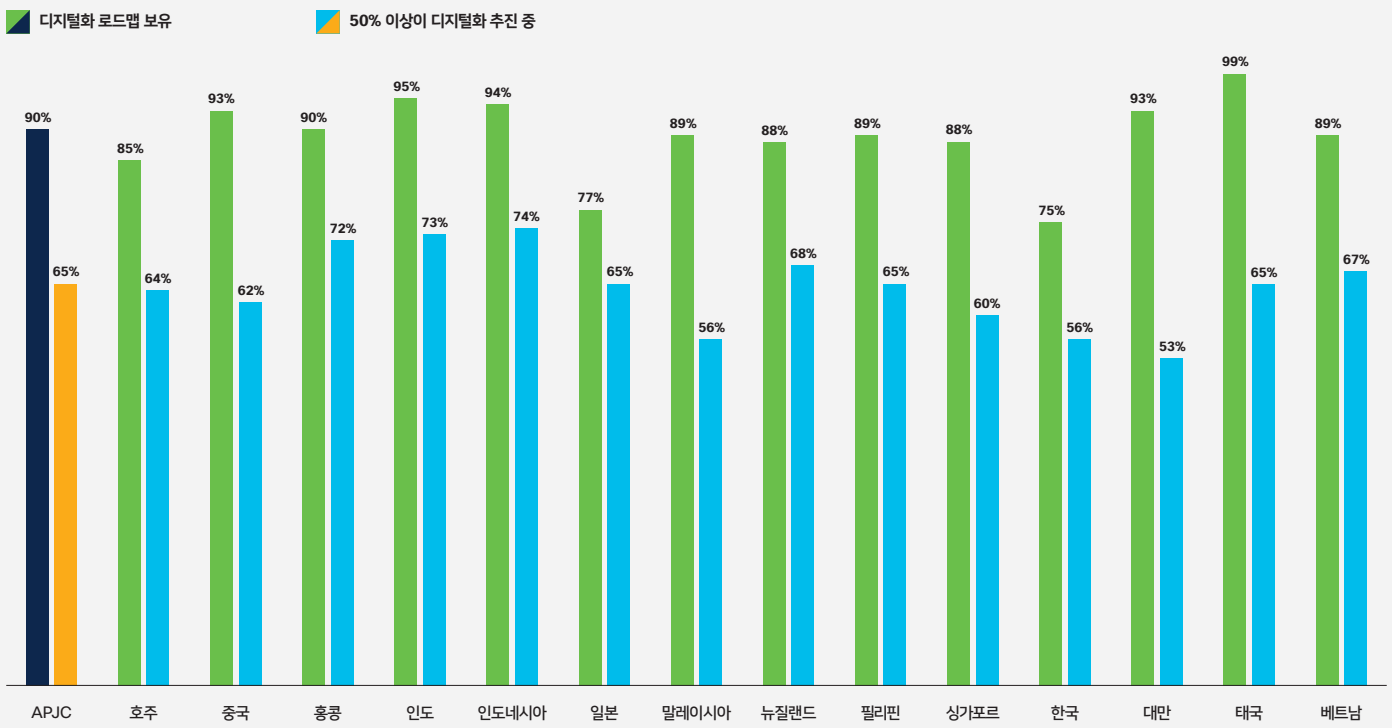
코로나 팬데믹으로 인해 모든 규모의 조직이 기술 솔루션 및 기능에 투자해야 할 필요성이 크게 증가했습니다. 팬데믹 초반에는 기업들이 생존을 위해 기술을 도입했습니다. 이는 모든 경제가 폐쇄 조치에 들어가고 대부분의 노동력이 원격 근무 환경으로 전환된 상황에서도 운영을 지속하고 고객에게 서비스를 제공하기 위한 것이었습니다. 하지만 기술이 가져다줄 수 있는 긍정적인 영향을 직접 목격하고 여러 국가에서 점차 경제 활동을 재개할 계획을 수립함에 따라, 모든 조직이 이제 기술을 활용하여 뉴 노멀 환경에서 성공하기를 바라고 있습니다.

특히 아시아 태평양 지역의 중소기업에게 이는 더욱 절실합니다. 시스코에서는 기술 트렌드, 특히 중소기업의 사이버 보안에 관련한 트렌드를 심층적으로 이해하기 위해 독립적인 연구를 의뢰했습니다.

연구 결과, 이 지역 중소기업의 94%가 새로운 기술을 도입한 것으로 나타났습니다. 더욱 고무적인 사실은 대부분(90%)이 디지털화 로드맵을 가지고 있다는 사실입니다. 특히 태국에서는 중소기업의 99%가, 인도에서는 95%가 로드맵을 가지고 있습니다. 하지만 일본, 한국과 같은 경제가 성숙한 국가에서는 이 수치가 다소 낮으며, 각각 중소기업의 77%와 75%가 디지털화 로드맵 또는 전략을 가지고 있다고 답했습니다.

실행 정도를 보면, 중소기업의 65%에서 어느 정도 디지털화가 진행된 상황이며, 디지털화 계획의 50% 넘게 배포를 완료했습니다. 인도네시아, 인도, 홍콩 특별행정구의 중소기업에서는 디지털화가 절반 이상 진행되었습니다. 반면 대만, 말레이시아, 한국의 디지털화가 가장 더딘 것으로 나타났습니다.

아시아 태평양 지역의 시장별 중소기업 디지털화 현황



아시아 태평양 지역의 중소기업의 디지털화가 가속화됨에 따라, 해커가 악용할 수 있는 공격 표면이 확대되고 악의적인 공격자가 디지털화의 속도를 따라오면서 중소기업은 사이버 보안에 더욱 주력하고 있습니다. 중소기업의 4분의 3이 12개월 전보다 현재 사이버 보안에 대한 우려가 커졌다고 답한 것은 놀라운 일이 아닙니다. 이는 상당한 비율이지만, 사이버 위협에 대한 중소기업의 인식이 높아졌음을 보여주기 때문에 바람직한 현상이기도 합니다.

이러한 우려에는 충분한 근거가 있습니다. 연구 결과, 아시아 태평양 지역 중소기업의 절반 이상(56%)이 지난해에 사이버 보안 사고를 경험했으며 다수가 사이버 범죄의 피해를 입었고 85%가 악성코드 공격을 당했습니다. 이러한 보안 사고의 결과로, 악의적인 공격자는 고객 정보(75%)부터 내부 이메일(62%), 직원 데이터(61%), 지적 재산(61%), 재무 정보(61%)까지 다양한 가치 있는 데이터를 획득하고 있습니다.

이는 중소기업에 실질적인 영향을 미쳐 응답자의 62%가 사이버 보안 사고로 인해 운영이 중단되었으며 61%가 수익 손실을 보았다고 답했습니다.

또한 57%가 고객의 신뢰를 잃었으며 66%는 사이버 보안 사고가 회사의 평판에 부정적인 영향을 미쳤다고 답했습니다. 수치화하긴 어렵지만, 평판과 신뢰의 하락은 모든 기업에 악영향을 끼칠 수 있습니다.

긍정적인 측면에서 보면 중소기업들은 이러한 당면 과제에 대해 인식하고 있습니다. 실제로 많은 중소기업에서 보안 태세를 파악하고 강화하기 위한 전략적 이니셔티브를 통해 이러한 당면 과제를 극복하기 위한 체계적인 접근 방식을 취하고 있습니다. 조사 결과, 81%가 지난 12개월간 잠재적인 사이버 보안 사고에 대한 시나리오를 기획하거나 그에 대한 시뮬레이션을 실행했습니다. 대부분(81%)이 대응 계획을 마련하고 있으며 82%는 필요한 경우 바로 실행할 수 있는 복구 계획을 가지고 있습니다. 시스코에서는 차후 보안 성과 연구를 통해 이 분야의 어떤 측면이 보안에 긍정적인 영향을 미치는지 심층적으로 측정할 예정입니다.

본 보고서가 아시아 태평양 지역 중소기업이 직면한 사이버 보안 당면 과제에 대한 유용한 인사이트가 되기를 바랍니다. 아시아 태평양 지역 중소기업은 직원들이 사무실 근무와 원격 근무를 오가게 되면서 사이버 보안 문제 해결이 더욱 복잡해짐에 따라 미래의 하이브리드 근무를 위한 대비를 하고 있습니다. 따라서 본 보고서의 모든 독자가 보고서에 제시된 실질적인 제안을 활용하여 사이버 준비 태세와 탄력성을 강화할 수 있기를 바랍니다.

점점 디지털화되는 세상에서는 모든 중소기업이 사이버 보안을 관리하고 강화하는 데 시간과 자원을 활용하여 기업의 탄력성을 높이고, 미래를 보장하며, 궁극적으로 성공을 만들어 가는 것이 더욱 중요합니다.

Kerry Singleton
시스코 아시아 태평양 지역 일본 및 중국, 사이버 보안 부문 상무이사

Michiko Kamata
시스코 아시아 태평양 지역 일본 및 중화권, 중소기업 성장 지부장

Bihan Roy
시스코 아시아 태평양 지역 일본 및 중화권, 상업기업 및 중견기업 부문 상무이사

소개

본 보고서에서는 아시아 태평양 지역 중소기업 3,700곳 이상에서 사이버 보안을 담당하는 비즈니스 및 IT 리더를 대상으로 실시한 설문 결과를 소개하고 분석합니다. 현장 조사는 2021년 4월부터 7월에 걸쳐 실시되었습니다.

이는 아시아 태평양 지역 중소기업이 직면한, 계속해서 변화하는 사이버 보안 당면 과제에 대한 심층적인 이해, 중소기업 리더가 사이버 대비에 접근하는 방식, 이를 개선하기 위한 제안을 제공하기 위한 것입니다.

설문은 호주, 중국, 홍콩, 인도, 인도네시아, 일본, 뉴질랜드, 말레이시아, 싱가포르, 한국, 대만, 태국, 필리핀, 베트남 등 아시아 태평양 지역 14개국을 대상으로 진행되었습니다.

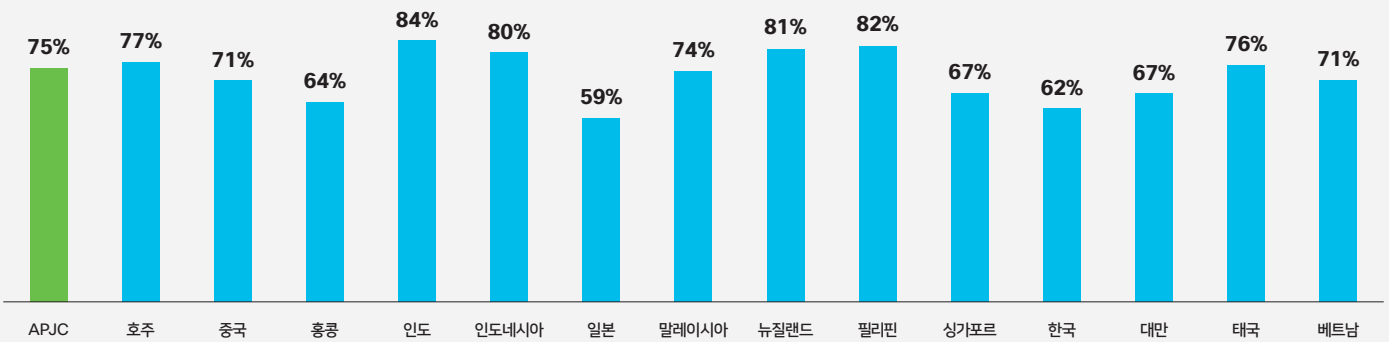
비즈니스 서비스, 건설, 교육, 엔지니어링, 설계 및 건축, 금융 서비스, 식음료, 의료, 제조, 미디어 및 커뮤니케이션, 천연자원, 퍼스널 케어 서비스, 전문 서비스, 부동산, 소매, 기술 서비스, 여행, 운송, 도매를 비롯한 다양한 산업의 대표적인 중소기업이 설문에 참여했습니다.

보안에 관한 우려

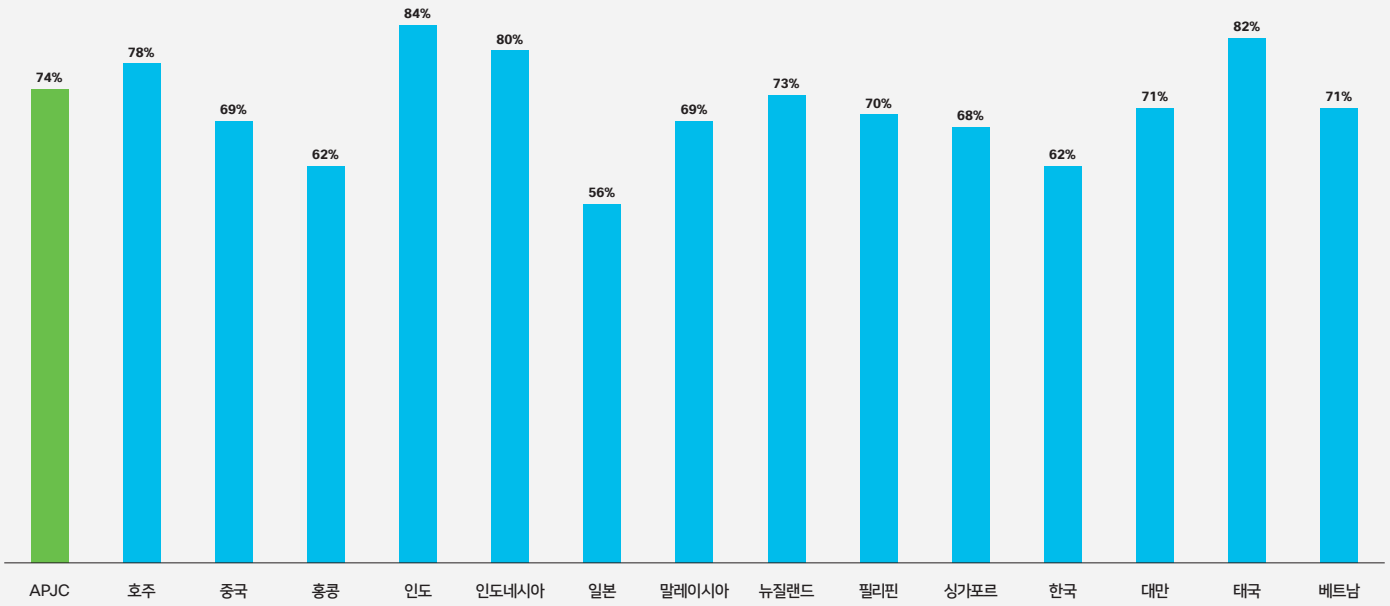
비즈니스 환경이 빠르게 변화함에 따라, 지난 한 해 동안 사이버 위협 환경도 크게 변화했습니다. 이에 따라 아시아 태평양 지역 중소기업들의 사이버 보안 위험에 대한 우려가 커졌습니다. 이 지역 중소기업의 4분의 3(75%)이 12개월 전보다 현재 사이버 보안에 대한 우려가 커졌다고 답했고, 그 비율은 인도(84%), 필리핀(82%), 뉴질랜드(81%), 인도네시아(80%), 호주(77%) 순으로 높았습니다.

이러한 우려의 이유 중 하나는, 심각한 보안 사고가 비즈니스에 미칠 수 있는 영향에 대한 인식이 높아지고 있기 때문입니다. 설문에 응답한 중소기업 리더의 4분의 3(74%)이 중대한 사이버 보안 사고로 인해 조직의 생명이 끝날 수 있다고 답했습니다.

12개월 전보다 현재 사이버 보안에 대한 우려가 커졌다고 답한 중소기업의 비율



심각한 사이버 보안 사고로 인해 비즈니스의 생명이 끝날 수 있다고 생각하는 중소기업의 비율

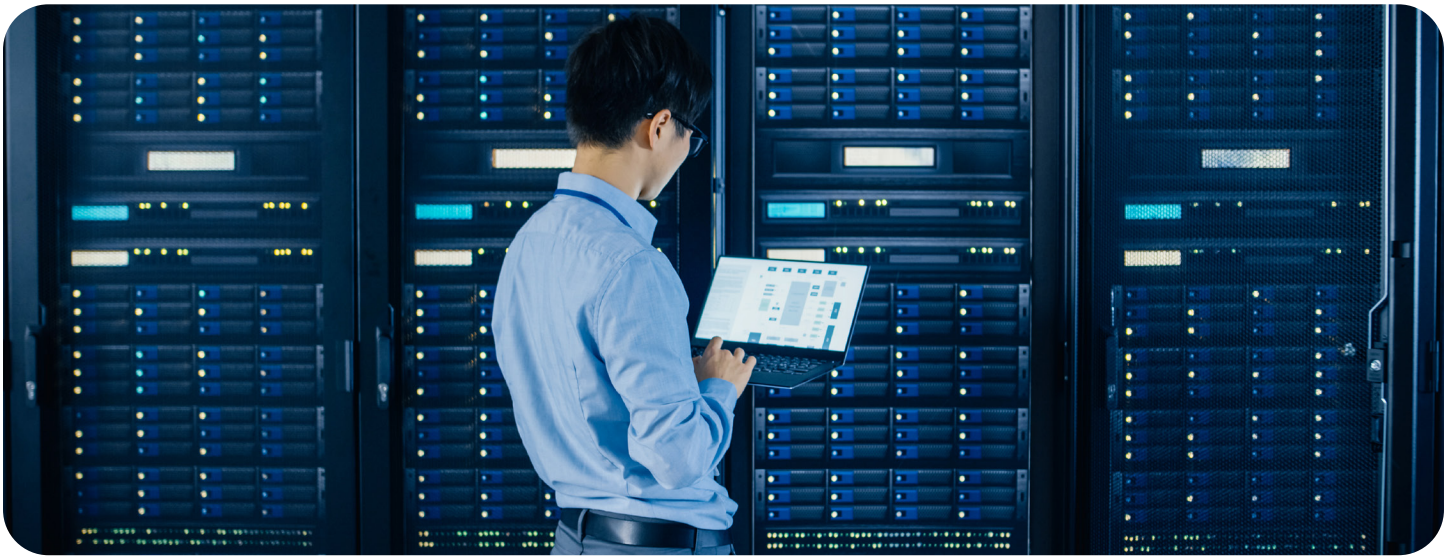


어디에서 가장 큰 위협이 발생하는 지에 대한 인식도 높아지고 있습니다. 조사 결과, 아시아 태평양 지역 중소기업의 43%가 가장 큰 위협으로 꼽은 피싱이 1위를 차지했습니다. 피싱은 해커가 신뢰할 수 있는 기관으로 가장하여 사용자가 전송된 이메일, 하이퍼링크 또는 인스턴트 메시지와 같은 특정 디지털 컨텐츠를 열도록 하는 기술입니다. 오래된 전략이지만 간단하고 효과적이기 때문에 여전히 많이 사용되고 있습니다.

한편 팬데믹으로 인해 빠르게 변화하는 환경에서 중소기업의 운영 방식에도 큰 변화가 있었습니다. 원격 근무로 대규모 전환됨에 따라, 많은 직원이 사무실 외부에서 회사 네트워크에 연결하고 정보에 액세스하고 있습니다. 이를 위해 개인 디바이스를 사용하는 경우도 많습니다. 중소기업들이 전반적인 보안에 대한 최대 위협이 되는 1위로 꼽은 것은 보안이 갖추어져 있지 않은 랩톱(20%), 악의적인 공격자의 타겟팅 공격(19%), 개인 디바이스(12%)의 순서였습니다.

다음 중 귀사 조직에 가장 큰 사이버 공격 위험은 무엇입니까?

노출 및 공격

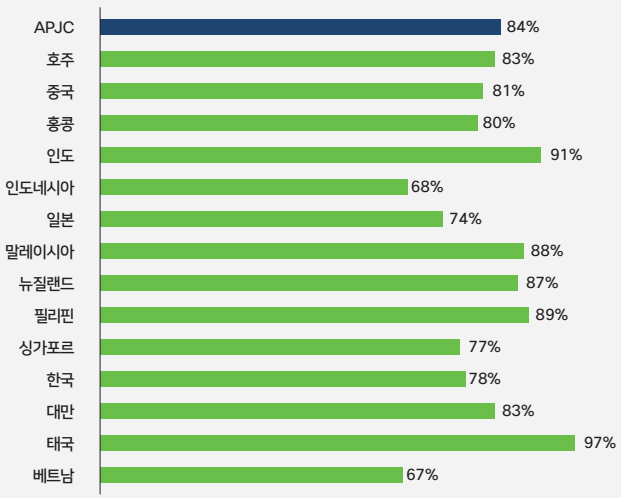


중소기업의 이러한 우려에는 충분한 근거가 있습니다. 아시아 태평양 지역 중소기업의 5분의 4 이상(84%)이 사이버 위협에 노출되어 있다고 생각하며, 3분의 1은 노출 정도가 심각하다고 생각합니다. 이는 특히 많은 중소기업이 사이버 보안 사고를 경험했기 때문입니다. 조사 결과 아시아 태평양 지역 중소기업의 56%가 지난 12개월 동안 사이버 보안 사고를 경험했습니다.

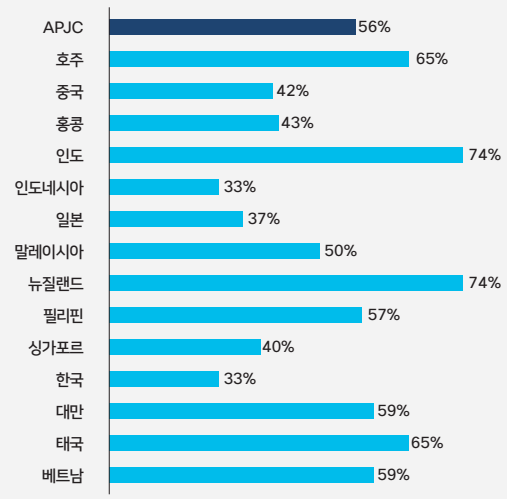
하지만 그 수치는 서로 크게 달라 인도와 뉴질랜드에서는 중소기업의 74%가 보안 사고를 경험한 반면 인도네시아와 한국에서는 33%, 일본에서는 37%만이 보안 사고를 경험했습니다.

또한 절반가량이 팬데믹 기간 동안 사이버 보안 사고가 증가했다고 답했습니다. 그중 인도(70%)와 뉴질랜드(61%)에서 증가율이 가장 높았고 필리핀(53%), 베트남(53%), 호주(50%)가 그 뒤를 이었습니다.

사이버 위협에 노출되었다고 생각하는 중소기업의 비율



최근 12개월간 사이버 보안 사고를 경험한 중소기업의 비율

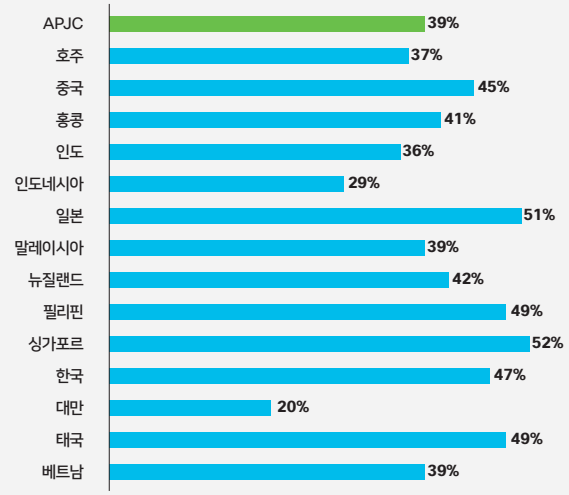


사이버 보안 사고를 경험한 중소기업 중 3분의 1(33%)이 가장 큰 이유로 사이버 보안 솔루션을 보유하고 있지 않다는 점을 들었습니다. 주목할 만한 점은, 이보다 많은 중소기업(39%)이 기존의 사이버 보안 솔루션으로는 공격을 감지하고 방지하기에 부족하다는 점을 최대 요인으로 꼽았다는 점입니다. 이를 통해 적합한 기술을 보유하는 것이 강력한 보안 태세를 구축하는 데 매우 중요하다는 사실을 알 수 있습니다. 이는 중소기업 부문을 심층적으로 조사한 시스코의 *보안 성과 연구*를 통해 도출된 주요 결과와도 일치합니다.

보안 사고를 경험한 중소기업들은 공격자가 시스템에 침투하는 다양한 방식을 확인했습니다. 중소기업의 85%에 영향을 준 악성코드 공격이 큰 부분을 차지합니다.

컴퓨터, 태블릿, 스마트폰과 같은 디바이스의 도입 및 사용량이 증가함에 따라 공격자들은 이러한 시스템에 대한 악성코드 배포를 더 많이 시도하고 있습니다.

사이버 보안 공격이 발생하는 가장 큰 요인을, 공격을 감지하고 예방하기에 충분치 않은 사이버 보안 솔루션 때문이라 응답한 비율



중소기업은 특히 대상으로 삼은 디바이스 성능을 저해하고, 손상을 입히며, 무단 액세스를 확보하기 위해 악의적인 소프트웨어를 배포하려는 공격자들의 타겟이 되고 있습니다.

공격자들이 중소기업을 대상으로 삼는 데는 몇 가지 이유가 있습니다. 첫째, 해킹 집단에는 중소기업이 대규모 조직에 비해 사이버 보안 측면에서 상대적으로 취약하기 때문에 매력적인 타겟이 된다는 인식이 있습니다. 둘째, 중소기업은 어떤 형태로든 대규모 기업과의 협력을 확대하고 있습니다. 해커들은 특정 중소기업 네트워크에 침투하면 이 네트워크를 발판 삼아 해당 중소기업과 협력하거나 디지털 트랜잭션 및 디지털 커뮤니케이션으로 연결된 대규모 기업의 네트워크에 액세스할 수 있을 것으로 생각합니다.

응답자들에 따르면, 악성코드 공격 후에는 피싱이 따릅니다. 70%가 이러한 공격을 경험했다고 답했습니다. 응답자들이 언급한 대표적인 기타 공격의 형태로는 DNS 터널링(68%), DoS(서비스 거부)(64%), SQL 삽입(62%), 끼어들기(61%), 제로데이 익스플로잇(60%)이 있습니다.

정의

DoS(서비스 거부) 공격: 일반적으로 은행, 미디어 회사 또는 정부 조직 웹 서버의 시스템 또는 네트워크를 종료하여 일반적인 사용자가 액세스할 수 없도록 함

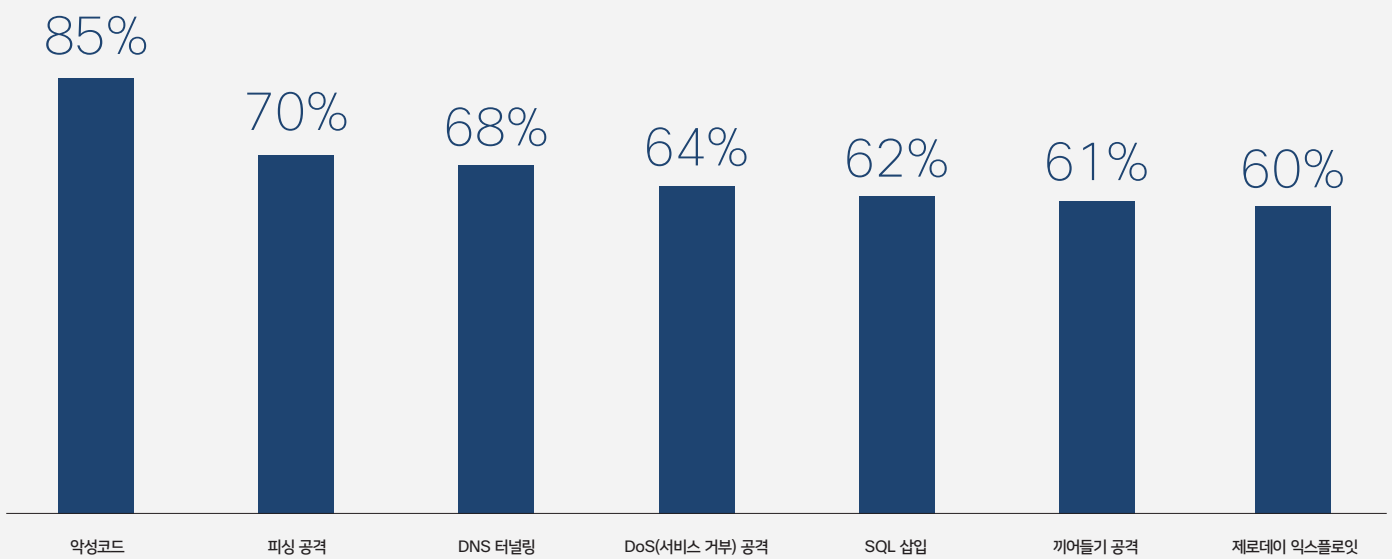
DNS 터널링: DNS 쿼리 및 응답 내 다른 프로그램 또는 프로토콜의 데이터를 인코딩함

SQL 삽입: 데이터 기반 애플리케이션 공격에 사용되며, 실행을 위한 항목 필드에 악의적인 SQL 문이 삽입됨(예: 데이터베이스 콘텐츠를 공격자에게 덤프)

끼어들기 공격: 공격자가 사용자와 애플리케이션 간의 대화에 끼어들어 정상적인 정보의 교환이 진행되고 있는 것처럼 보이도록 만든 다음 개인 정보를 훔침

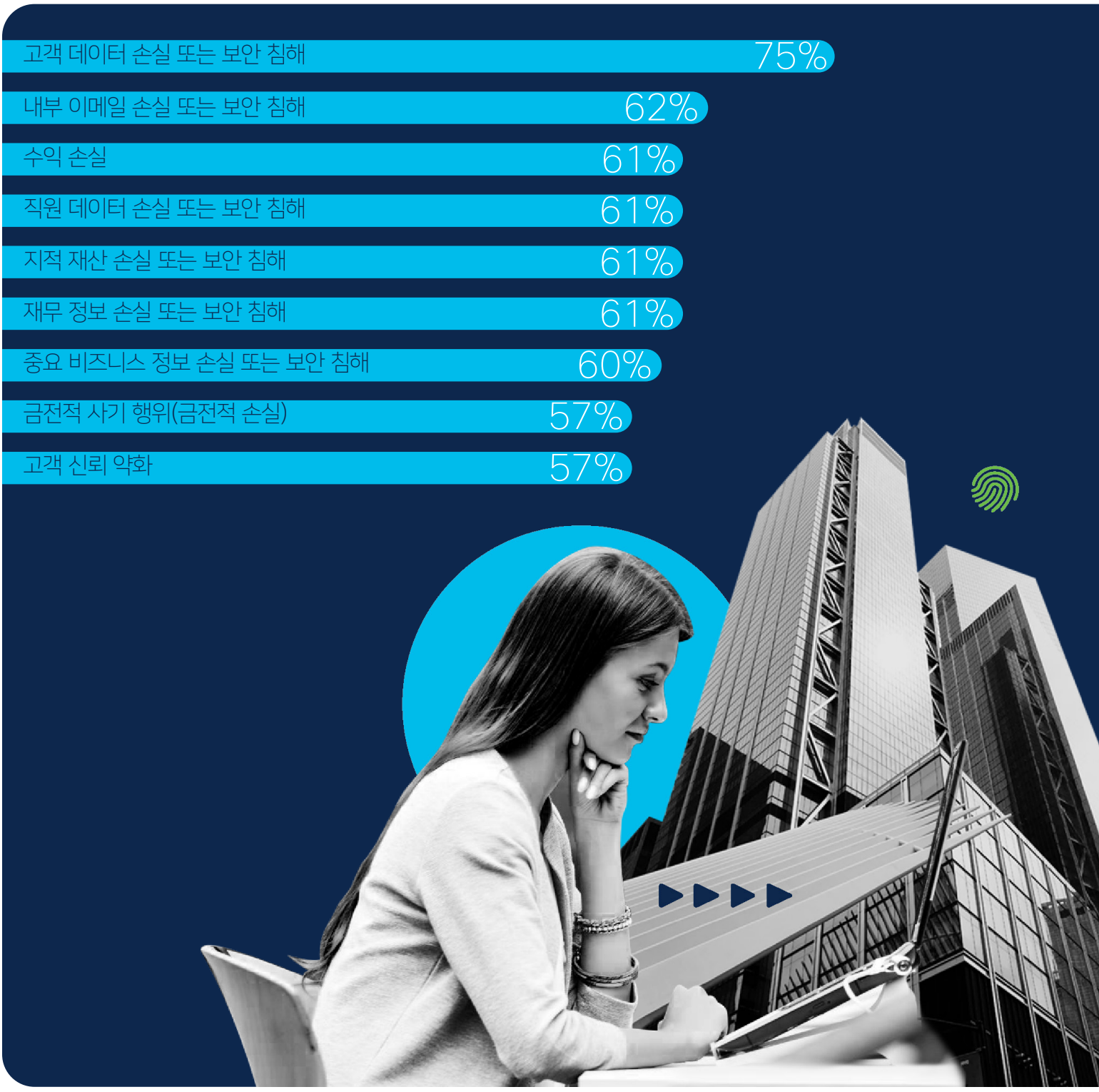
제로데이 익스플로잇: 최근에 발견된 소프트웨어 취약점을 공격하여 데이터를 훔치거나 손상을 일으키는 공격

아시아 태평양 지역 중소기업이 지난 12개월간 경험한 사이버 보안 사고의 유형



비용 계산

보안 사고를 경험한 중소기업의 대부분에 다양한 형태의 손실이 발생했습니다.
보안 사고를 경험한 중소기업의 무려 75%가 고객 데이터 손실이 발생했다고 답했습니다. 보안 사고를 경험한 중소기업 10곳 중 6곳이 수익에 부정적인 영향이 발생했다고 답했습니다.



매 순간 비즈니스에 영향을 미치는 사이버 보안

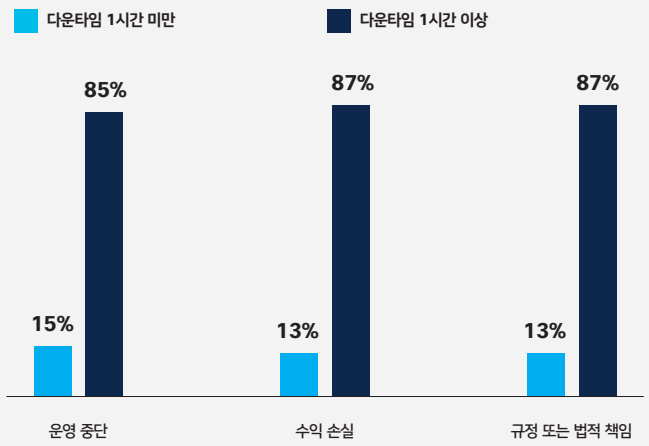
사이버 보안은 확률 게임입니다. 하지만 현실적으로 확률은 악의적인 공격자에게 유리합니다. 이들은 타겟을 끊임없이 공격하고 있습니다. 공격을 받는 대상은 매번 이겨야 합니다. 반면 공격자는 한 번만 방어를 뚫으면 이길 수 있습니다.

기업이 사이버 보안 사고를 감지, 조사, 해결하는 데에는 어느 정도 시간이 걸린다는 점도 한몫을 합니다. 이에 따라 악의적인 공격자가 한발 앞서 손상을 일으킬 수 있게 되는 경우가 많습니다.

현재 중소기업의 당면 과제는, 우리가 고객이 즉각적인 만족을 원하는 고도로 연결된 디지털 우선 세계에 살고 있다는 점입니다. 따라서 중소기업은 사이버 보안 사고로 인해 운영이 방해받는 일을 막아야 합니다. 그들은 사이버 보안 사고를 최대한 빠르게 감지, 조사, 차단, 해결할 수 있어야 합니다.

아시아 태평양 지역 중소기업의 약 10분의 9(85%)가 어떤 부문이라도 1시간 이상의 다운타임이 발생하면 운영이 중단된다고 답했습니다. 응답자의 87%가 어디에라도 1시간 이상의 다운타임이 발생하면 수익 손실이 발생한다고 답해 그 영향을 수량화할 수 있습니다. 주목할 만한 점은, 중소기업의 10분의 3(29%)이 1일 이상의 다운타임이 발생하면 조직 운영이 중단될 것으로 답했다는 사실입니다.

다운타임의 시간에 따른 영향의 증가*



* 각 측정항목의 시장별 분석은 부록 A 차트를 참조하시기 바랍니다.

또한 많은 국가에서 사이버 보안 지침과 규정을 도입하고 시행하기 시작함에 따라, 사이버 보안 사고로 인해 다운타임이 발생하면 법적인 책임이 따릅니다. 이미 이러한 트렌드가 나타나기 시작하고 있으며, 중소기업의 87%가 1시간 이상의 다운타임이 발생하면 법적인 책임이 따른다고 답했습니다.

설문에 참여한 응답자의 15%만이 1시간 이내에 사이버 보안 사고를 감지할 수 있다고 답했다는 사실을 보면 이러한 트렌드가 중소기업에 얼마나 큰 당면 과제인지 알 수 있습니다. 1시간 이내에 보안 사고를 해결할 수 있는 중소기업의 비율은 이보다도 낮은 10%에 불과합니다. 아시아 태평양 지역 조직의 절반 이상(55%)이 보안 사고를 감지하는 데 2시간 넘게 걸렸으며, 45%가 2시간 이내에

최근 12개월간 사이버 보안 사고를 경험한 중소기업

	APJC	호주	중국	홍콩	인도	인도네시아	일본	말레이시아	뉴질랜드	필리핀	싱가포르	한국	대만	태국	베트남
보안 사고 감지에 소요되는 평균 시간															
1시간 미만	15%	8%	13%	11%	17%	17%	16%	17%	24%	9%	8%	11%	25%	13%	8%
1시간 이상	84%	93%	86%	88%	83%	84%	84%	83%	77%	89%	91%	89%	76%	86%	91%
조직에서 보안 사고를 해결하는 데 소요된 평균 시간															
1시간 미만	10%	6%	8%	3%	12%	12%	9%	12%	11%	9%	5%	4%	16%	7%	3%
1시간 이상	90%	95%	91%	96%	87%	89%	91%	88%	90%	90%	95%	97%	83%	92%	96%

보안 사고에 대응할 수 있었습니다. 느린 대응이 비즈니스에 미칠 수 있는 영향을 고려했을 때 보안 사고에 대한 대응 속도는 매우 중요합니다.

중소기업이 처리해야 하는 문제는 수익 손실만이 아닙니다. 사이버 보안 사고는 전반적으로 금전적인 영향도 미칩니다. 지난 12개월 동안 사이버 보안 사고를 경험한 아시아 태평양 지역 중소기업의 절반 이상(51%)이 이로 인해 50만 달러 이상의 비용이 발생했다고 답했으며, 13%는 100만 달러가 넘는 비용이 발생했다고 답했습니다.

실제로 보안 사고를 경험한 중소기업 대부분에 금전적 영향이 발생했습니다. 전체적으로 83%가 10만 달러가 넘는 비용이 발생했다고 답했습니다.

눈에 보이지 않는 비용도 있습니다. 지난해에 보안 사고를 경험한 중소기업의 57%가 고객의 신뢰를 잃었다고 답했고, 66%가 평판에 부정적인 영향이 발생했다고 답했습니다. 수치화하긴 어렵지만, 평판과 신뢰의 하락은 모든 기업에 악영향을 끼칠 수 있습니다.

지난 12개월간 사이버 보안 사고의 재정적 영향(US$)

	APJC	호주	중국	홍콩	인도	인도네시아	일본	말레이시아	뉴질랜드	필리핀	싱가포르	한국	대만	태국	베트남
50만 달러 이상	51%	64%	41%	39%	62%	43%	49%	32%	62%	28%	51%	58%	27%	47%	30%
100만 달러 이상	13%	33%	3%	10%	13%	12%	6%	6%	18%	10%	11%	10%	2%	28%	4%

대비를 통한 두려움 극복

사이버 보안 사고에 대한 우려와 실질적인 영향에도 불구하고, 아시아 태평양 지역 중소기업은 포기하지 않고 극복하기 위한 대비를 하고 있습니다. 이들은 기획과 교육을 시작하여 응답자의 81%가 시나리오 계획 및/또는 시뮬레이션을 완료했다고 답했습니다.

현실적인 시나리오 계획을 수립하고 시뮬레이션을 수행하면 특히 공격자가 취약점을 악용하기 전에 보안 태세의 취약점을 파악할 수 있기 때문에 이러한 계획 및 시뮬레이션은 사이버 대비 태세를 갖추는 데 핵심적인 역할을 합니다. 시뮬레이션을 실시한 아시아 태평양 지역 중소기업 중 85%가 사이버 방어의 취약점 또는 문제점을 발견했다고 답했습니다.

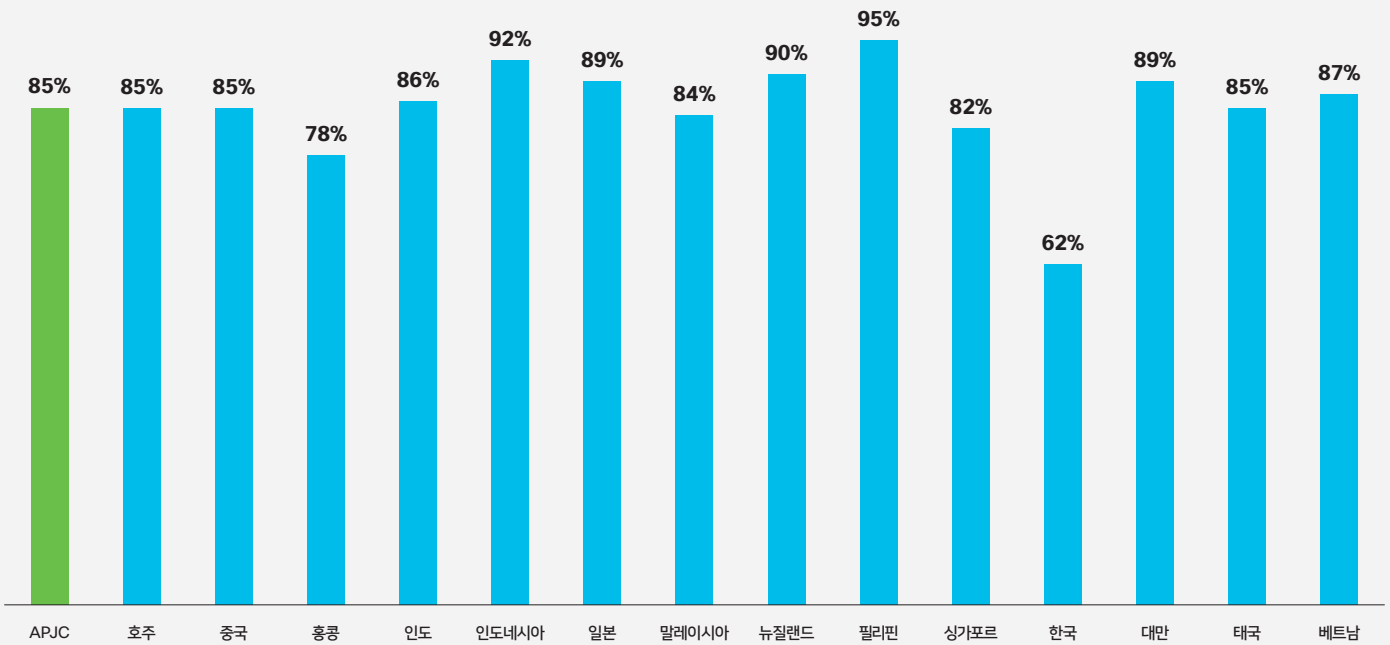
취약점을 파악한 중소기업 중 95%가 이러한 활동을 통해 사이버 공격 또는 위협을 감지하기에 적합한 기술 솔루션을 갖추지 못한 문제가 드러났다고 답했습니다. 동일한 비율의 중소기업이 보유한 기술이 너무 많아 통합에 어려움을 겪은 반면 96%는 공격을 차단하는 데 적합한 기술 솔루션이 없다는 사실을 알게 되었다고 답했습니다.

사이버 공격에 대한 대응 프로세스가 명확하지 않다는 사실이 드러났다고 답한 비율도 높았습니다(94%). 한편 95%는 적합한 기술을 보유하고 있었지만 이러한 기술을 활용할 수 있는 역량을 갖춘 직원이 충분하지 않았다고 답했습니다.

중소기업의 약 절반 정도가 두 주 내에 시나리오 계획을 통해 파악한 격차 또는 문제를 해결할 수 있었다는 점은 고무적입니다. 유일한 예외는 공격 또는 위협 감지에 적합한 기술을 보유하고 있지 않다는 문제를 발견한 중소기업으로, 이들 대부분은 이러한 문제 해결에 더 많은 시간이 소요되었습니다.

아시아 태평양 지역 중소기업들은 사이버 보안 측면의 탄력성을 강화하기 위해 적합한 시나리오 기획의 단계를 밟고 있지만, 다른 영역에서도 해야 할 일이 있습니다. 대표적인 과제 중 하나는 모든 관계자에 대한 교육입니다. 약 5분의 1(17%)의 응답자가 경영진이 해당 국가의 사이버 보안 법률 및 규정 요건에 대한 이해가 부족하다고 답했습니다. 이러한 지식 격차는 뉴질랜드(30%), 홍콩(29%), 일본(28%), 한국(27%)에서 더욱 두드러집니다.

사이버 보안 시나리오 기획 및/또는 시뮬레이션을 통해 사이버 방어의 취약점이 드러났습니까? (그렇다고 답한 비율)



투자 관리 및 수익 창출

또한 중소기업은 투자를 통해 대비 계획을 지원하고 있습니다. 실제로 조사 결과 아시아 태평양 지역에서 사이버 보안에 대한 투자의 수준이 높은 것으로 나타났습니다.

아시아 태평양 지역 중소기업의 3분의 2(63%)가 사이버 보안에 평균적으로 연간 수익의 4% 이상을 지출하며, 30%는 6% 이상, 9%는 10% 이상을 지출합니다.

실제로, 아시아 태평양 지역 중소기업의 약 4분의 3이 팬데믹이 시작된 이후로 사이버 보안에 대한 투자를 확대했으며, 5분의 2는 투자액을 5% 이상 증대했습니다.

주목할 만한 점은, 증가한 지출이 여러 핵심 영역에 걸쳐 고르게 분배되었다는 점입니다. 이는 강력한 사이버 보안 태세 구축에 대한 다차원적인 통합 접근 방식의 필요성을 강하게 인식하고 있음을 보여줍니다.

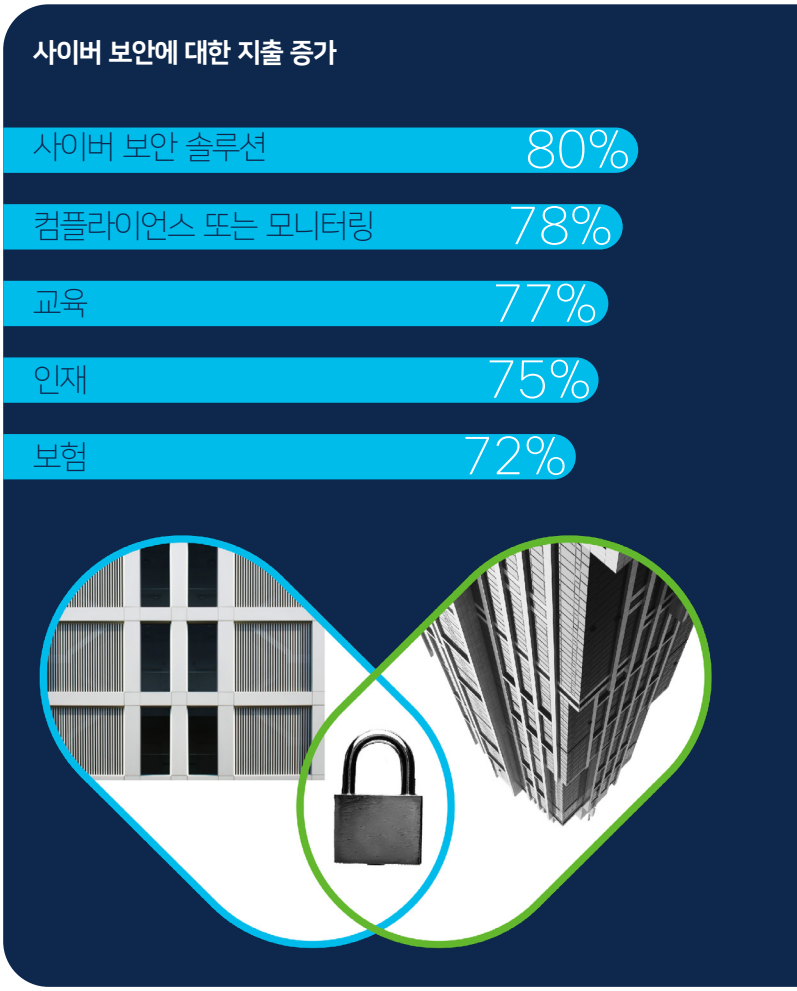
연간 수익 중 사이버 보안에 대한 평균 지출 비율

	APJC	호주	중국	홍콩	인도	인도네시아	일본	말레이시아	뉴질랜드	필리핀	싱가포르	한국	대만	태국	베트남
없음	1%	1%	0%	2%	1%	1%	8%	0%	0%	1%	2%	3%	0%	1%	0%
1% 미만	8%	11%	4%	7%	6%	5%	18%	13%	17%	7%	9%	15%	13%	6%	2%
1-3%	27%	27%	30%	38%	20%	14%	33%	28%	26%	32%	29%	37%	42%	19%	18%
4-5%	33%	34%	45%	40%	30%	37%	29%	23%	24%	32%	36%	28%	24%	32%	53%
6-10%	21%	15%	15%	9%	30%	34%	9%	24%	21%	14%	17%	15%	17%	27%	16%
10% 초과	9%	11%	6%	3%	13%	9%	3%	12%	11%	15%	7%	2%	4%	15%	11%

당면 과제의 경우, 중소기업들은 계속해서 진화하는 기술과 보안 요구 사항에 발맞추는 것(77%), 끊임없이 진화하는 사이버 위협의 속도를 따라가는 것(76%), 직원들의 책임 있는 참여를 유도하는 것(75%), 업계의 지나친 복잡성(75%), 채용 역량(73%)이 사이버 보안 탄력성을 강화하는 데 가장 큰 걸림돌이라고 답했습니다.

오른쪽과 같이, 아시아 태평양 지역 중소기업이 충분한 사이버 보안 태세를 구축하려면 솔루션, 컴플라이언스, 인재, 교육과 같은 영역에 대한 투자를 확대해야 합니다.

중소기업들이 보안 대비 태세를 전체적인 관점에서 바라보고 있다는 사실을 통해 사이버 보안에 대한 인식이 제고되고 있음을 잘 알 수 있습니다. 하지만 솔루션, 인재, 교육에 대한 투자에도 불구하고 중소기업들은 사이버 공격에 대해 불리한 입장에 있습니다. 이는 업계의 특성일 뿐입니다. 사이버 보안 사고가 비즈니스에 미치는 잠재적인 영향에 대한 인식이 점차 높아지고 법적인 책임이 확대됨에 따라, 중소기업들은 사이버 보안 보험에 적극적으로 투자하고 있습니다. 이를 통해 보안 사고가 발생하는 경우 비즈니스에 미칠 수 있는 재정적 영향을 완화할 수 있습니다.



다음 요인을 사이버 보안 탄력성 향상에 대한 걸림돌로 보는 중소기업의 비율

	APJC	호주	중국	홍콩	인도	인도네시아	일본	말레이시아	뉴질랜드	필리핀	싱가포르	한국	대만	태국	베트남
진화하는 기술 및 보안 요구 사항에 발맞추는 것	77%	82%	63%	73%	87%	53%	69%	84%	83%	89%	79%	75%	72%	71%	80%
진화하는 사이버 위협의 속도를 따라가는 것	76%	80%	59%	71%	87%	50%	66%	87%	81%	88%	82%	74%	74%	77%	81%
직원들의 책임 있는 참여를 유도하는 것	75%	76%	61%	65%	86%	55%	70%	81%	82%	81%	75%	67%	68%	73%	81%
업계의 지나친 복잡성	75%	77%	61%	63%	85%	57%	65%	80%	87%	82%	82%	69%	65%	74%	79%

중소기업 보안을 위한 5가지 관행

본 보고서에서는 계속해서 변화하는 사이버 보안 환경에서 중소기업들이 공통으로 가지고 있는 당면 과제를 알아봅니다. 본 섹션에서는 모든 규모의 중소기업이 사이버 보안 태세를 강화할 수 있는 5가지 관행을 소개합니다.

1 **소통:** 사이버 보안 환경은 끊임없이 진화하고 있기 때문에 중소기업은 위협과 조직에 미치는 잠재적인 영향을 파악해야 합니다. 고위급 경영진과 모든 관계자가 참여하는 정기 회의를 자주 개최하면 비즈니스 기획에 위협 환경을 반영할 수 있습니다. 사이버 보안 이벤트를 처리하기에 충분한 역량을 갖춘 중소기업은 이러한 문제에 대해 자주 의견을 나눕니다. 이러한 기업 중 90% 이상이 매주, 3분의 2(68%)가 매일 이러한 문제에 대해 소통을 합니다. 위협에 맞설 준비가 비교적 미흡한 중소기업들은 이러한 소통의 빈도가 낮아, 약 3분의 1(31%)이 한 달에 한 번 이하로 문제를 논의합니다.

2 **단순성:** 사이버 보안 해결에 대한 기존의 접근 방식은 당장 특정 문제를 해결하기 위해 포인트 보안 제품 및 솔루션을 구매하는 것입니다. 하지만 이로 인해 많은 중소기업에서 인프라에 서로 통합되지 않은 제품과 솔루션이 너무 많아져 운영이 복잡해지고 사이버 보안 사고가 발생하는 경우 원하지 않는 지연이 발생하고 있습니다. 사이버 보안 스택의 다양한 부분 간 상호 운용성을 평가하는 것은 공격에 대처하는 속도와 결과에 대단히 중요합니다. 개별 제품 및 솔루션을 서로 연결하려면 보안 인프라 전체에 대한 명확한 가시성을 확보하고 시스템을 실제 상황에서 테스트할 때 원활하게 작동할 수 있도록 통합 플랫폼 접근 방식이 필요합니다.

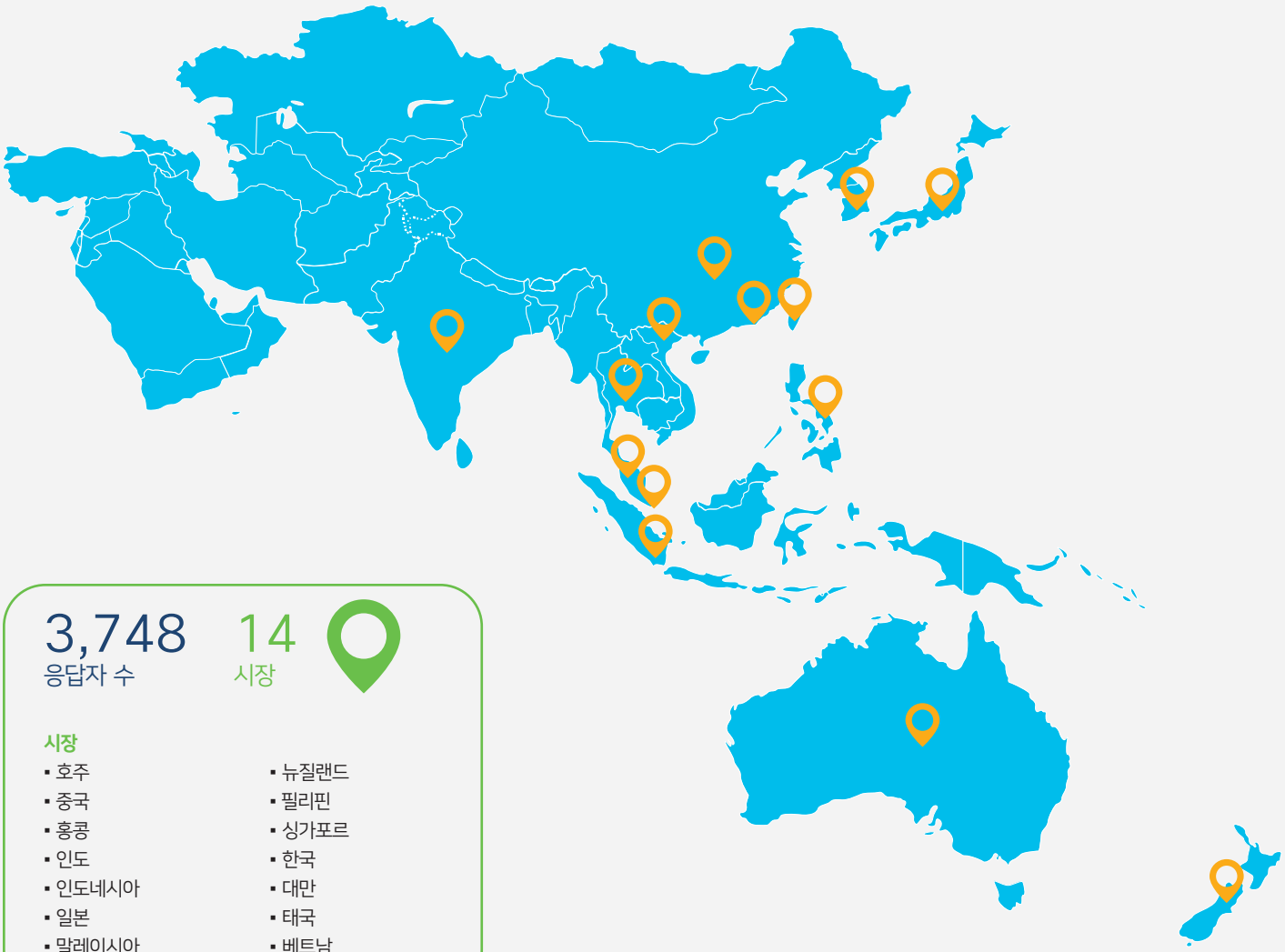
3 **성패를 좌우하는 준비 태세:** 중소기업이 실제 상황에 대한 대비를 갖출 수 있는 방법 중 하나는 더욱 통제된 환경에서 상황과 결과를 시뮬레이션하는 것입니다. 이를 통해 중소기업은 취약점이 어디인지 실질적으로 파악하고 이를 해결할 수 있는 기회를 얻으며 보안 사고가 발생하는 실제 상황에 더욱 효과적으로 대비할 수 있습니다. 실제로 연구 결과, 효과적인 대비를 갖춘 중소기업의 공통적인 특성 중 하나는 98% 이상이 지난 12개월 이내에 시나리오 기획 또는 시뮬레이션을 수행했다는 점입니다. 이들 중 대부분인 96%가 최대한 빠르고 효율적으로 비즈니스의 운영 연속성을 유지하기 위한 복구 계획을 수립했습니다. 반대로, 효과적인 기획을 하지 않은 중소기업 중 절반 이상(58%)이 시나리오 기획을 수행하지 않았고 약 3분의 2(63%)가 복구 계획을 수립하지 않았습니다.

4 **교육:** 중소기업이 구축할 수 있는 모든 기술 및 솔루션 중에서, 사람이 가장 약한 연결 고리가 되는 경우가 많다는 점을 이해해야 합니다. 사이버 보안 부문의 괄목할 만한 발전에도 불구하고, 피싱(기본적으로, 수신된 디지털 커뮤니케이션 컨텐츠에 포함된 링크를 클릭하도록 사람들을 유도하는 것)이 계속해서 가장 큰 위협 벡터 자리를 유지하고 있다는 사실을 통해 이를 확인할 수 있습니다. 중소기업은 직무에 관계없이 전 직원이 사이버 보안과 비즈니스의 안전을 보호하는 데 있어 자신이 기여할 수 있는 역할에 대한 기본적인 이해를 갖추도록 해야 합니다.

연구 결과 나타난 데이터에 따르면 이 부분이 취약한 것으로 드러났습니다. 사이버 보안 환경 관리에 대한 효과적인 대비를 갖춘 중소기업 중 96%가 직원들이 사이버 보안에 대한 전체적인 이해를 갖추고 있다는 데 동의했으며, 95%가 잠재적인 공격의 심각성과 자신의 역할을 이해한다고 답했습니다. 이와 반대로 보안 이벤트에 대한 대비가 부족한 중소기업들은 직원들에 대한 신뢰도가 낮아, 15%만이 직원들이 사이버 보안에 대해 이해하고 있다는 데 동의했습니다.

5 **협력:** 적합한 기술 파트너와의 협력은 사이버 보안 측면에서의 전반적인 성공을 달성하는 데 중요합니다. 중소기업이 명심해야 할 사항은 다음과 같습니다. 첫째, 비즈니스 전체를 아우르는 엔드-투-엔드 보호를 제공할 수 있는 역량을 갖춘 파트너와 협력해야 합니다. 대부분의 경우, 이를 위해서는 여러 제품과 솔루션을 하나의 플랫폼으로 통합하여 인프라 전체에 단순성과 가시성을 제공해야 합니다. 둘째, 중소기업들이 디지털화에 착수함에 따라 비즈니스가 성장하게 되면서 운영이 확장될 것입니다. 따라서 규모에 상관없이 운영을 보호할 수 있는 역량을 갖춘 파트너와 협력해야 합니다. 마지막으로, 파트너는 중소기업이 원하는 기술 구축 방식에 따라 다양한 사용 모델을 제공할 수 있는 역량을 갖추어야 합니다.

본 연구에 관한 정보



3,748
응답자 수

14
시장

시장
- 호주
- 중국
- 홍콩
- 인도
- 인도네시아
- 일본
- 말레이시아
- 뉴질랜드
- 필리핀
- 싱가포르
- 한국
- 대만
- 태국
- 베트남

대상
사이버 보안을 담당하는 IT 및 비즈니스 리더

참여 조직 구성:
- 중소기업(직원 수 1명 ~ 249명)
- 중견기업(직원 수 250명 ~ 999명)

업종
- 광고 또는 시장 조사
- 비즈니스 서비스(예: 회계, 컨설팅)
- 건설
- 교육
- 엔지니어링, 설계, 건축
- 금융 서비스
- 의료
- 제조
- 미디어 및 커뮤니케이션
- 천연자원(예: 석유, 광업, 삼림업)
- 퍼스널 케어 서비스
- 전문 서비스
- 부동산
- 레스토랑 서비스
- 소매
- 기술 서비스
- 운송
- 여행 서비스
- 도매
- 기타

부록 A

다운타임의 길이에 따른 영향의 증가

	APJC	호주	중국	홍콩	인도	인도네시아	일본	말레이시아	뉴질랜드	필리핀	싱가포르	한국	대만	태국	베트남
조직 운영에 심각한 영향이 발생하기 전까지 가능한 다운타임 시간															
1시간 미만	15%	10%	21%	11%	17%	18%	10%	13%	17%	16%	7%	10%	21%	18%	8%
1시간 이상	85%	90%	79%	89%	83%	83%	90%	87%	83%	84%	92%	90%	79%	81%	93%
수익에 심각한 영향이 발생하기 전까지 가능한 다운타임 시간															
1시간 미만	13%	8%	16%	12%	12%	25%	7%	16%	9%	15%	10%	14%	14%	14%	9%
1시간 이상	87%	92%	83%	88%	88%	75%	93%	85%	91%	85%	89%	87%	85%	86%	92%
규정 또는 법적 책임이 발생하기 전까지 가능한 다운타임 시간															
1시간 미만	13%	7%	16%	14%	13%	19%	6%	17%	8%	13%	11%	13%	18%	14%	12%
1시간 이상	87%	94%	84%	86%	86%	81%	95%	84%	93%	86%	89%	88%	80%	86%	89%

Cisco Secure 소개

오랫동안 네트워크 분야의 선도 업체로서 명성을 쌓아 온 시스코는 사이버 보안 솔루션으로 구성된 개방적인 통합 포트폴리오를 보유하고 있습니다. 보안 솔루션은 서로 연동되면서 시너지 효과를 발휘할 수 있도록 설계해야 합니다. 이러한 솔루션은 서로 학습해야 하며,

잘 통합된 하나의 공동체로 운영되고 위협에 대처할 수 있어야 합니다. 이 모든 것이 갖추어졌을 때, 보안은 보다 체계적이고 효과적일 수 있습니다. 시스코는 오랫동안 고객들에게 세계 최대의 IT 인프라 및 네트워크 서비스 공급자이자 세계 최대의 B2B 사이버 보안 기업으로 인정받았습니다.

오직 최고의 보안을 추구한다는 원칙으로 탄생한 Cisco Secure는 고객 중심의 합리적인 보안 방식으로 배포, 관리 및 사용이 간편할 뿐 아니라 모든 기능이 서로 연동되면서 시너지 효과를 발휘합니다. 사람, 즉 고객이 모든 비즈니스의 중심이 되어야 한다는 것이 시스코의 경영 원칙입니다. 그리고 시스코는 복잡하고 귀찮은 문제를 해소하고, 확실한 보안 관행으로 실질적인 성과를 거두고자 하는 고객의 희망을 잘 알고 있습니다. 그러려면 보안을 간소화하되, 간소한 보안 뒤에 복잡한 계산이 깔려 있어야 합니다. 시스코의 클라우드 네이티브 플랫폼은 바로 이런 부분에서 획기적인 성과를 발휘합니다.

시스코 Cisco SecureX 플랫폼은 현재는 물론 미래의 위협까지 안전하게 막아 준다는 신뢰와 확신을 보안 커뮤니티에 선사합니다. Fortune 100대 기업으로 선정된 모든 기업에서 지구상에서 가장 포괄적이고 통합된 시스코 사이버 보안 플랫폼으로 비즈니스의 현재와 미래를 보호하고 있다는 사실이 그 증거입니다. 간소한 보안 환경에서 성공을 앞당기고 미래를 보장받는 방법을 자세히 알아보려면 cisco.com/go/secure를 참조하세요.

시스코 보안 성과 연구

더욱 자세한 내용은 2021 Security Outcomes Study for Small to Midsize Businesses(SMB)를 참조하시고 자세한 Cisco Secure 사고 리더십 콘텐츠 전용 페이지를 방문하시기 바랍니다.

미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam
The Netherlands

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 **https://www.cisco.com/go/offices**에서 확인하십시오.


CISCO