Cisco 사이버 보안 보고서 시리즈 2020

중견·중소 기업(Small and Medium-Sized Business: SMB)

cisco Secure

소규모 비즈니스 세계의 큰 보안

중견·중소 기업(SMB) 사이버 보안에 관한 **10가지** 통념 깨뜨리기

cisco The bridge to possible

목차

사이버 보안이 여러분의 조직을 의도한 대로 보호하고 있습니까?

중견·중소 기업(SMB라고도 함)을 운영하고 있거나, 중견·중소 기업에서 근무하는 경우 이미 상당한 당면 과제를 극복했을 것입니다. 종자돈을 모으고 고용 시기를 파악하는 것부터 운영 비용을 관리하고 확장 전략을 마련하는 데 이르기까지... 신경 쓸 일이 많습니다. 신나고, 의미 있고, 보람이 있지만... 힘듭니다.

감염병이 유행하는 시기나 경제 불황을 겪는 것처럼 전례가 없는 상황에 직면할 때 이를 어떻게 관리합니까? 보안 유지를 위해 무엇에 주력해야 합니까? 직원이 감축된 상태에서 운영할 때 사이버 공격으로부터 조직을 어떻게 보호합니까?

이러한 기업가로서의 본능이 꿈틀대기 시작합니다. 위기 상황이 발생하면 필요에 따라 새로운 접근 방식에 적응하면서 새로운 아이디어가 등장합니다. 온갖 악조건 속에서 생산성과 경쟁력을 유지하는 방법을 떠올리게 됩니다.

고려해야 할 다른 급한 문제가 있을 때 사이버 보안이 중요한 역할을 담당합니까?

분명 그럴 것입니다! 이 보고서는 사이버 보안이 중소 규모 조직의 생존뿐 아니라 빠른 발전 및 성공에 있어 얼마나 중요한 역할을 할 수 있는지에 관한 인사이트를 제공합니다. 그 인사이트를 제공하는 방법은? 바로 데이터를 사용하여 중견·중소 기업 보안에 관해 만연한 잘못된 통념을 깨는 것입니다.

지금까지 중견·중소 기업이 사이버 보안에 적절한 우선순위를 부여하는 것에 대한 보안 업계의 인식은 부당할 정도로 부정적인 경우가 많았습니다. 보안을 심각하게 여기지 않는다는 가정 하에 벤더가 중견·중소 기업에 영합하고 장황한 설명만 늘어놓는 것("사이버스플레이닝"이라고도 함)처럼 보였을 것입니다.

거의 500곳에 달하는 중견·중소 기업(직원 수 250 ~ 499명인 기업)을 대상으로 조사한 이 보고서는 중견·중소 기업이 보안을 매우 중시할 뿐만 아니라, 이들의 보안에 대한 혁신적이고 진취적인 접근 방식도 효과적인 것으로 나타났습니다. 이제 중견·중소 기업이 사이버 보안 리소스를 사용하는 방식에 대한 잘못된 통념을 바로잡아야 합니다.

연례 CISO 벤치마크 설문 조사 결과와 중견·중소 기업들과의 대화를 활용하여 사전적 위협 추적을 전담하는 부서를 보유한 SMB의 수, 직면하게 될 사이버 위협의 유형 등에 관해 만연하는 통념을 파헤칠 것입니다.

즉, 사이버 보안에 영향을 미치는 주요 요인을 자세히 살펴볼 것입니다. 예를 들어, 오래된 인프라가 보안 침해에 미칠 수 있는 결과와 이것이 얼마나 지속될지에 관해 알아봤습니다. 또한 사용하는 벤더가 많을 수록 가장 심각한 보안 침해로 인해 다운타임이 길어진다는 것을 알았습니다. 가장 영향력 있는 전략을 살펴보고, 업계에서 이전에 예상했던 것보다 데이터 보안 침해가 발생한 후에도 기업이 더욱 빠르게 복구된다는 것을 보여주는 데이터를 보여줄 것입니다.

중견·중소 기업으로서 겪는 모든 어려움에 더해, 이제는 외부의 요인으로 인해 인력 중 일부 또는 전체가 언제든 원격으로 근무해야 하는 상황이 될 수 있습니다. 독립적 사이버 보안 분석가이자 블로거인 Graham Cluley는 최근 자신의 뉴스레터에서 "집에서 근무할 수는 있지만 해킹은 계속해서 발생한다"고 언급했습니다. 예전과는 다른 업무 방식으로 적응해야 할 수도 있으며, 어려운 시기에는 우선순위를 정하는 것이 필수입니다.

이 보고서의 목표는 어떤 전략이 효과적인지에 관해 집중하는 것입니다. 향후 기업과 소속 직원들이 보안 관리 방법을 정하고 비즈니스 성공의 가속화를 위해 사이버 보안 솔루션을 선택할 때, 이 보고서를 통해 의사 결정 과정에서 도움을 받으시길 바랍니다.

"보안은 조직에서 중요한 역할을 합니다. 저희는 미국 내 3개 신용 조합은 물론 통합 콜 센터의 백엔드 기능을 수행합니다. 보안은 비즈니스의 주요 요소를 통합하여 운영 효율성을 높이는 데 도움이 됩니다."

Kevin Hatch, 네트워크 엔지니어,
Open Technology Solutions

10가지 통념 살펴보기

중견·중소 기업과 대기업의 보안 태세 비교

중견·중소 기업 보안 태세에 관한 일반적인 통념을 평가하기 위해 중견·중소 기업(직원 수 250~499명)와 대규모 조직(직원 수 500명 이상)의 다양한 사이버 보안 기능에 대한 설문 조사 응답을 비교했습니다.

연구 데이터에서 확인한 바에 따르면 여러 가지 통념이 깨졌습니다. 여기에서는 이러한 통념을 조사하고 틀렸음을 입증하는 데이터를 제공하여 중견·중소 기업의 보안 태세가 생각보다 뛰어남을 증명합니다.

참고:

1. 이번 연구의 목적을 위해 중견·중소 기업(SMB)은 직원 수가 250~499명인 기업으로 정의했습니다. 직원 수가 250명 미만인 조직의 설문 조사 데이터는 다를 수 있음에 유의하십시오.
2. 모든 백분율은 반올림 처리되었으며, "모른다" 답변의 경우 그 비율이 적어 생략했습니다. 이러한 이유로 제공된 그래프에서 백분율의 총합이 100%가 되지 않을 수 있습니다. 설문 조사 데이터 출처: Cisco 2020 CISO 벤치마크 연구

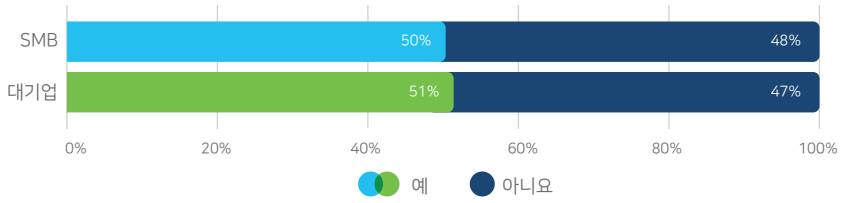
통념 1: 대규모 조직만이 모든 형태의 공개 조사를 받는다

일반적인 통념 중 하나는 미디어에서 대기업 또는 정부 데이터 보안 침해에 대해서만 이야기하고자 한다는 것입니다. 이로 인해 일부 소규모 조직은 사이버 공격을 겪더라도 공개 조사를 받지 않을 것이라 믿을 수 있습니다.

그렇지 않습니다. 지난 해 중견·중소 기업은 대기업과 동일한 수준의 공개 조사를 받았습니다.

그림 1은 공개 조사 여부에 있어 중견·중소 기업과 대기업의 차이가 있다는 증거가 없음을 보여줍니다.

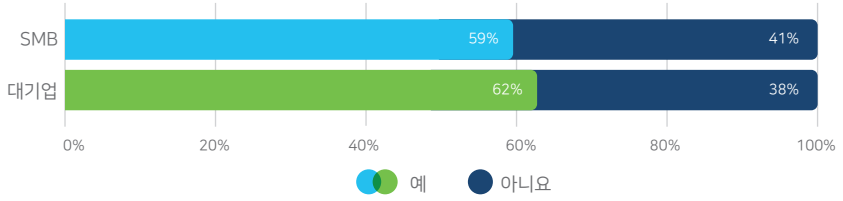
그림 1. 여러분의 조직에서는 보안 침해에 대한 공개 조사를 받았던 적이 있습니까? SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

두 번째로 중견·중소 기업의 59%는 지난 해 가장 중대한 데이터 보안 침해를 자발적으로 공개했습니다(대기업의 경우 62%). 이는 중견·중소 기업이 고객 및 파트너에게 책임감 있는 자세를 보이고 있음을 암시합니다.

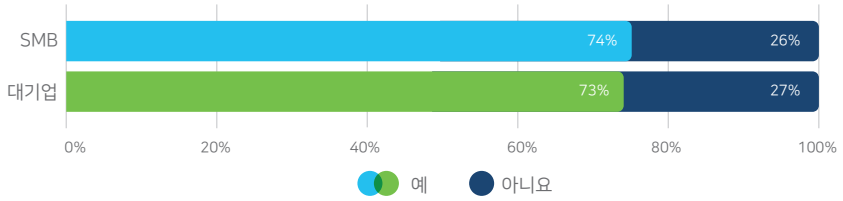
그림 2. 지난해 공개 조사 관리 대상이 된 중대 보안 침해 사례가 발생했으며, 그 사실이 조직의 자발적 공개로 인해 일반에 알려진 적이 있습니까? SMB N=241, 500+ N=1190.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

세 번째, 중견·중소 기업이 고객으로부터 데이터 처리 방법에 관한 질문을 받는 경우가 받지 않는 경우보다 훨씬 많습니다. 중견·중소 기업의 74%가 고객/잠재 고객이 이러한 질문을 한 적이 있다고 답했습니다(73%인 대기업과 비슷한 결과). 이를 통해 고객은 어디에서 개인 데이터를 보유하는지와 무관하게 개인 데이터의 안전을 걱정하고, 이러한 안전을 제공하는 신뢰 요소가 분명하게 중요함을 알 수 있습니다.

그림 3. 고객(또는 잠재 고객)이 데이터 프라이버시와 개인 정보 처리 방식에 관해 질문합니까? SMB N=432, 500+ N=2117.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

중견·중소 기업에서 이러한 질문을 받는 이유는 규제와 벤더 위험 관리 체계가 위에서 아래로 흐르기 때문입니다. 시작은 대기업입니다. 그런 다음 대기업은 그들의 벤더인 중간 규모 기업을 감사합니다. 몇 년 후에는 중간 규모 조직들이 그들의 벤더인 소규모 기업을 감사합니다. 보안 침해 또는 데이터 프라이버시로 인해 중견·중소 기업 역시 이러한 질문에 예외일 수 없습니다. 대기업 못지 않게 책임을 가져야 하는 셈입니다.

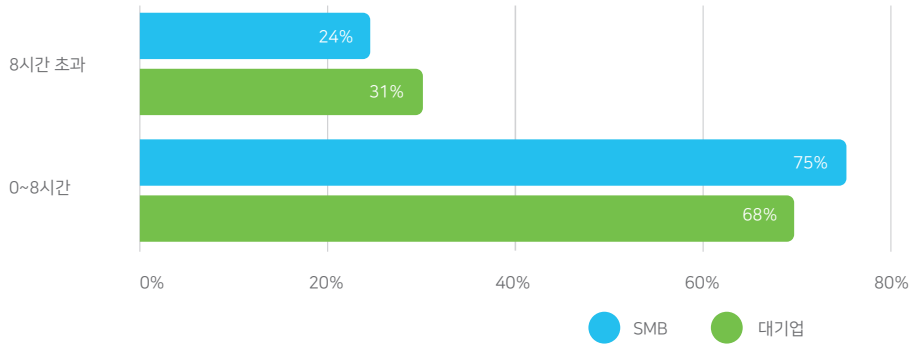
통념 2: 대기업은 다운타임 피해가 적고 공격으로부터 빠르게 복구된다

중견·중소 기업이 사이버 공격을 받아 다운타임이 발생할 때(업무 시간 손실) 대기업 못지않은 빠른 속도로 복구하기에 리소스가 충분하지 않다는 통념이 있습니다.

그렇지 않습니다. Cisco의 데이터에 따르면 중견·중소 기업과 대기업이 겪는 다운타임의 규모는 큰 차이가 없습니다.

결과 중 일부를 요약하자면 중견·중소 기업의 24%는 지난 해 가장 심각한 보안 침해로 인해 8시간을 초과하는 다운타임이 발생했으며, 이는 31%인 대기업보다 약간 낮은 수치입니다.

그림 4. 지난 1년 간 조직이 경험한 가장 심각한 보안 침해가 발생했을 때 이 보안 침해로 인해 발생한 시스템 다운타임은 어느 정도였습니까? SMB N=388, 500+ N=1877.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

또한 이 수치를 2018년 Cisco의 "Small and Mighty" 중견·중소 기업 보고서와 비교했는데, 지난 2년 동안 중견·중소 기업에서 몇 가지 큰 발전이 이루어졌습니다. 2년 전에는 중견·중소 기업의 40%가 가장 심각한 보안 침해가 발생한 이후 8시간을 초과하는 다운타임이 발생했습니다.

여기에서 기업의 규모와 무관하게 심각한 보안 침해로 인해 대규모의 중단이 발생할 수 있음을 인정해야 합니다. 중요한 것은 어디의 다운타임이 긴가가 아니라 역량 내에서 리소스가 유지되도록 중견·중소 기업에서 어떤 조치를 취할 수 있는가입니다. 여기에서 자동화가 힘든 시기에 다운타임을 최소화하고 비즈니스를 유지할 수 있도록 조기 경보와 빠른 복구를 제공하는 전력 증강자가 될 수 있습니다. 2020 CISO 벤치마크 보고서에 따르면 모든 규모의 조직에서 다수(77%)가 앞으로 보안 에코시스템의 응답 속도를 높이고 이를 간소화하기 위해 자동화를 강화할 계획이라고 응답합니다.

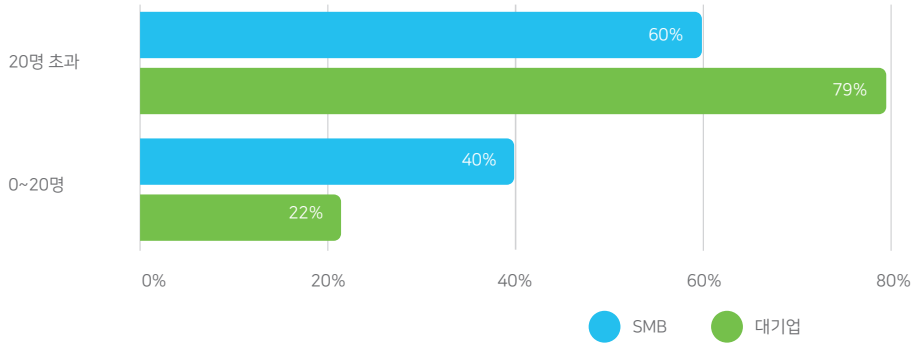
통념 3: 중견·중소 기업은 보안 전문 인력이 부족하다

모두가 중견·중소 기업에 필요한 것이 무엇인지 고민할 때 사이버 보안은 본인이 아닌 다른 누군가의 책임이라고 가정합니다. 게다가 그 누군가가 데이터 센터 관리 및 새 하드웨어 평가와 같은 다른 IT 관리 업무와의 균형을 맞춘다고 생각합니다. 중견·중소 기업에는 사이버 보안 전문 자원이 부족하다는 통념이 있습니다.

그렇지 않습니다. 일부의 경우일 수 있지만 많은 중견·중소 기업에서 사이버 보안 전담 직원이 있다고 답했습니다. 실제로 중견·중소 기업 가운데 보안 전담 직원이 없다고 답한 중견·중소 기업은 1%도 되지 않습니다. 더욱 놀라운 사실은 비록 업무 수준 또는 해당 직원이 MSSP(Managed Security Service Provider)로부터 아웃소싱되었는지 여부에 대해 명시하지 않았지만 60%가 보안 전담 직원이 20명 이상이라고 답했다는 것입니다.

그렇다면 대기업과 비교한다면 어떨까요? 보안 전담 직원이 20명 이상인 대기업의 비율은 예상대로 79%라는 높은 수치를 기록했습니다.

그림 5. 조직 내에 보안 전담 직원 수는 몇 명입니까? SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

이러한 수치는 처음에 생각했던 것보다 중견·중소 기업에는 보안 전담 리소스의 수가 더 많음을 보여줍니다. 이는 사이버 보안 인력 부족이 더 이상 중견·중소 기업의 문제가 아님을 의미할까요?

그렇게까지 단정지을 수는 없습니다.

중견·중소 기업에서는 숙련된 인력 부족이 실제로 세 번째로 큰 당면 과제라고 답했습니다. 가장 큰 당면 과제는 예산 부족이며, 그 다음은 레거시 시스템과의 호환성입니다. 세 번째가 숙련된 인력과 경쟁 우위입니다.

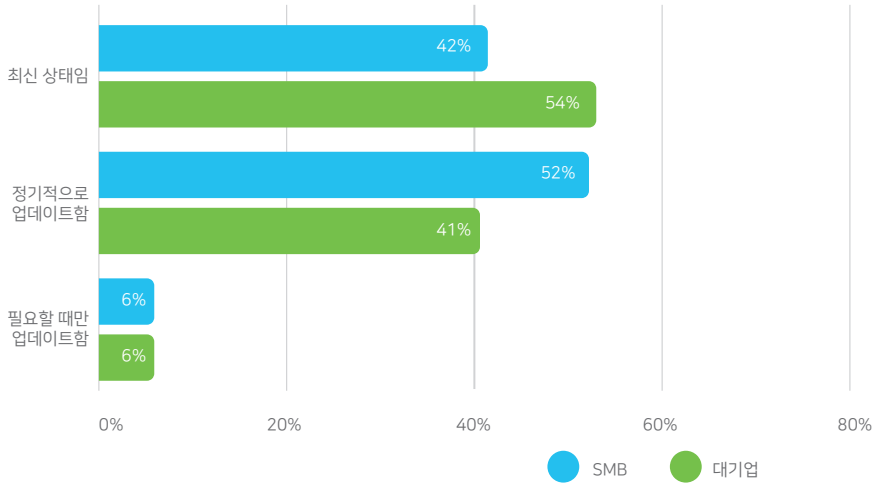
이를 통해 중견·중소 기업 역시 사이버 보안 문제를 겪고 있음을 알 수 있습니다. 중견·중소 기업 역시 공격 목표이며, 이들을 향한 공격 역시 점점 정교해지고 있습니다. 여기에 대응하기 위해 중견·중소 기업은 가급적 최적의 위치에 서려 합니다. 중견·중소 기업 조직에 있어 이는 적절한 인력에게 투자하는 것을 의미합니다.

통념 4: 대기업이 더 많은 최신 인프라를 보유한다

더 많은 소비자들이 최신 스마트폰으로 업그레이드하는 가운데 대기업은 보안 인프라의 각 요소를 대체할 수 있는 것처럼 보일 수 있습니다. 하지만 순환식 투자가 연간 IT 예산에 더 큰 영향을 미칠 수 있는 중견·중소 기업의 경우는 어떻습니까?

부분적으로 사실입니다. 인프라와 주요 보안 기술 투자 및 교체 전략을 설명해 달라고 요청했을 때 중견·중소 기업의 답변은 다음과 같았습니다. 거의 모든 중견·중소 기업이 꾸준하게 인프라를 최신 상태로 유지하고 있습니다.

그림 6. 조직의 보안 인프라를 어떻게 설명하시겠습니까? SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

중견·중소 기업의 경우 최신 상태인 인프라가 대기업보다 적은 것이 사실입니다(최신 상태라고 답한 대기업은 54%, 중견·중소 기업의 경우 42%). 하지만 전부 합하여 중견·중소 기업의 94%가 정기적으로 또는 지속적으로 인프라를 업데이트한다고 답했습니다. 따라서 대다수는 노후하고 안전하지 않은 상태가 될 때까지 오래된 장비를 그대로 보유하지 않는다는 것이 분명합니다.

중견·중소 기업의 경우 완전히 새로운 보안 제품을 보유하려는 것 대신 현재의 보안 제품을 극대화하는 것이 중요합니다. 중견·중소 기업 고객들이 독창적인 아이디어를 통해 보안을 강화하려는 것을 여러 차례 목격했습니다.

"저희 회사와 같은 중견·중소 기업은 가능한 한 적은 시스템에서 최대한 많은 정보를 수집하여 효율성을 극대화해야 합니다. Cisco의 클라우드 기반 보안 솔루션(Cisco AMP for Endpoints)은 전체 인프라를 운영하는 데 매우 중요한 시스템으로 입증되었습니다. 이 솔루션은 에셋을 안전하게 보호할 뿐만 아니라 시스템의 정보, 사용자 환경 및 헬프 데스크에서의 문제 해결을 지원하는 보고에 즉시 액세스하는 기능도 제공합니다. 따라서 별도의 소프트웨어 시스템을 사용할 필요가 없습니다. 이러한 방식으로 운영하여 계속 학습하고 조정할 수 있습니다."

Alan Zaccario, New Castle Hotels and Resort의 정보 기술 및 사이버 보안 부문 부사장

통념 5: 중견·중소 기업은 대기업과는 다른 유형의 위협에 직면한다

사이버 범죄자들은 더 큰 보상을 원하기에 대기업을 상대로 가장 은밀하고 위험한 전략을 사용할 것입니다. 맞습니까?

어느 정도는 맞습니다. Cisco에서는 중견·중소 기업과 대기업이 지난 해에 경험한 것으로 보고한 사이버 공격의 유형과 그 공격으로 인한 다운타임(업무 시간 손실)이 어느 정도인지 비교했습니다. 직원 수를 기준으로 한 4개의 범주를 사용하여 비교한 다음 24시간을 초과하는 다운타임이 발생할 가능성이 가장 높은 이벤트 순위를 매겼습니다.

그림 7. 지난 1년 동안 가장 심각한 보안 침해 때문에 발생한 다운타임 및 그 원인인 공격 유형과 직원 수 사이의 상관 관계. 250-499 N=388, 500-999 N=746, 1,000-9,999 N=863, 10,000+ N=268.

출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

어떤 위협이 가장 큰 피해를 입혔는지에 있어 흥미로운 결과가 나왔습니다. 랜섬웨어는 대기업과 중견·중소 기업을 차별하지 않았습니다. 중견·중소 기업 및 대기업의 경우 24시간을 초과하는 시스템 다운타임의 가장 큰 원인이 바로 랜섬웨어였습니다.

DDoS의 경우 중견·중소 기업에는 큰 영향을 미치지 않았지만 직원이 10,000명 이상인 기업에 있어서는 세 번째로 위협적인 공격 유형이었습니다. 반대로 피싱은 규모가 작은 조직에서 큰 문제였던 것으로 보고된 반면 규모가 큰 조직에서는 적절하게 대처되었습니다.

와이퍼 악성코드를 구축하는 공격자의 유일한 목적은 시스템 및/또는 데이터의 파괴 또는 방해입니다. 중견·중소 기업과 직원이 10,000명 이상인 대기업 모두에 있어 와이퍼 악성코드는 지난 해 17~24시간의 다운타임을 유발했습니다. 데이터를 두고 몸값을 요구하는 악성코드(랜섬웨어)와 달리 악의를 가진 해커가 와이퍼를 사용하기로 결정하는 데 있어 금전적인 동기는 없습니다. 기업에 있어서는 데이터 복구를 전혀 기대할 수 없기에 이는 최악의 공격인 경우가 많습니다.

자격 증명 도용 역시 중견·중소 기업에서는 중대한 문제였는데, 지난 해 평균 17~24시간의 다운타임을 유발했습니다.

또한 일부 위협 행위자는 특정 규모, 분야 또는 지리적 위치의 기업을 중점적으로 공략하는 것에 주목해야 합니다. 따라서 전술은 (이전 수치에 표시된 것과 같이) 비교가 가능할 수 있지만 위협 행위자는 하나하나가 서로 다릅니다.

통념 6: 중견·중소 기업은 사전적으로 위협 추적을 하지 않는다

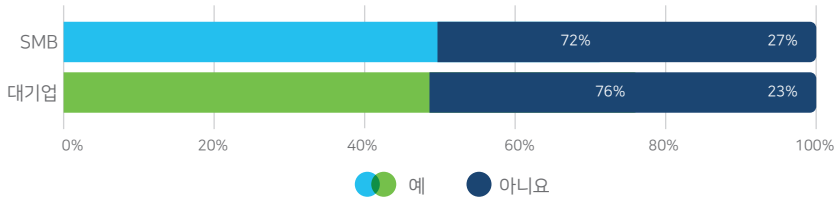
위협 추적은 사전적인 보안 조치로, 환경에 침투하고 경보도 울리지 않은 공격자를 찾아내 없애는 것을 목표로 합니다. 이는 잠재적으로 악의적인 활동이 탐지된 후에 표시되는 경보에서 시작하는 기존 조사 및 대응 방식과는 대조됩니다.

위협 추적의 전반적인 개념을 들어보면 중견·중소 기업의 역량을 벗어나는 복잡성을 가진 미스테리 사건 현장을 조사하는 것과 같습니다. 중견·중소 기업은 경보를 조사하는 데 최선을 다하지만 다른 위협을 추적할 시간적 여유는 없습니다. 그렇지 않습니까?

그렇지 않습니다. 설문 조사 데이터에 따르면 중견·중소 기업의 72%가 위협 추적 전담 직원을 보유하고 있으며, 이는 위협 추적 부서를 보유한 대기업의 비율과 비슷합니다.

리소스 부족으로 인해 대기업에 비하면 그 수준은 차이가 날 수 있지만 데이터에 따르면 중견·중소 기업은 사이버 보안에 대한 사전 접근 방식의 가치를 인지하고 이를 수용하고 있습니다.

그림 8. 조직에 위협 추적을 전담하는 내부 부서 또는 팀이 있습니까? SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

최신 보고서인 숨겨진 위협 추적: 보안 프로그램에 위협 추적 통합에서 위협 추적의 사례와 다른 비즈니스에서 이를 어떻게 수행하는지 자세히 알아볼 수 있습니다.

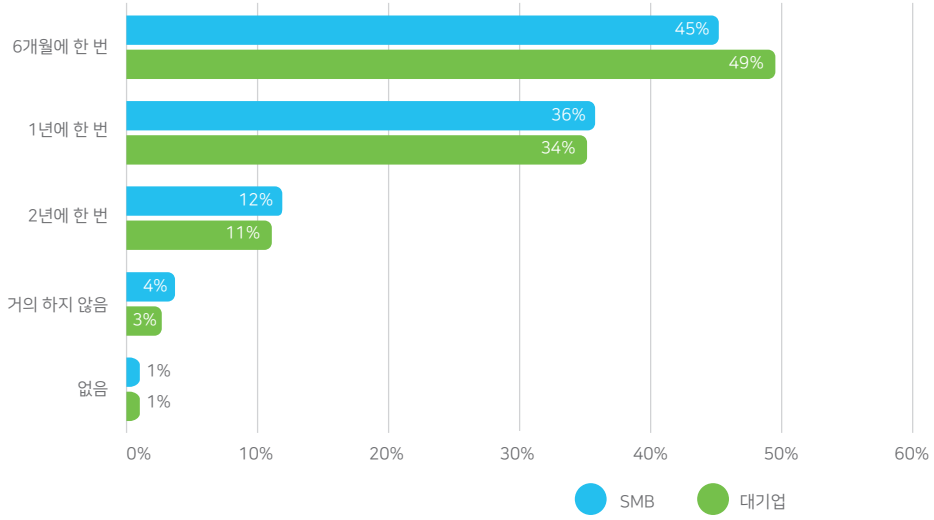
통념 7: 규모가 작은 기업은 훈련/연습을 통해 사고 대응 계획을 테스트하지 않는다

Mike Tyson은 이런 말을 남겼습니다. "모두가 계획을 가지고 있다. 실제로 얼굴에 주먹을 맞기 전까지는." 사고 대응 계획은 실제로 어떻게 진행되는지 알기 전까지 그저 종이에 적힌 글에 불과합니다.

하지만 중견·중소 기업의 경우 그 계획을 테스트할 시간과 리소스가 부족합니다. 그렇지 않습니까? 실제로 테스트의 가치보다는 중단되는 시간이 너무나 소중할 것입니다.

하지만 그 통념은 전혀 사실이 아닙니다. 중견·중소 기업의 1%만이 계획을 테스트한 적이 없으며, 거의 테스트하지 않는다고 답한 비율도 4%에 불과합니다. 21%가 2년마다 테스트를 하고, 매년 테스트를 하는 중견·중소 기업은 36%에 달합니다. 그리고 6개월마다 테스트한다는 답변이 가장 많았습니다(45%).

그림 9. 사이버 보안 사고에 대한 회사의 대응 계획을 테스트하기 위해 조직에서 훈련이나 연습을 수행하는 빈도는? SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

그렇다면 대기업과 비교한다면 어떨까요? 결과는 매우 비슷합니다. 따라서 중견·중소 기업이 사고 대응에 있어 대기업만큼 계획을 세우지 않는다는 통념이 깨졌습니다.

통념 8: 이유가 어떻든 중견·중소 기업 리더십은 보안과 데이터 프라이버시를 심각하게 여기지 않는다

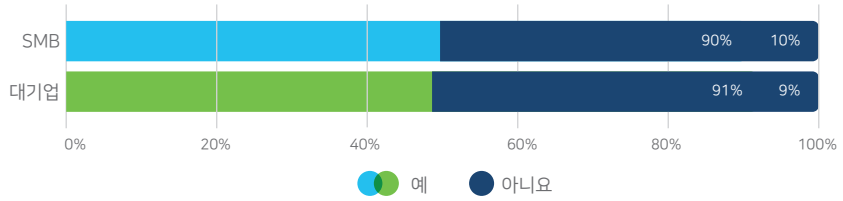
오랜 시간 동안 업계 전체에 퍼진 큰 통념입니다. 중견·중소 기업은 얼마나 큰 위험이 도사리고 있는지 알지 못하며, 보안과 데이터 프라이버시에 관한 조직 문화도 성숙하지 않았습니다.

그렇지 않습니다. 데이터에 따르면 이러한 통념은 실제 사실과 많이 다릅니다. 각기 다른 규모의 조직에 속하는 IT 의사 결정권자들의 답변을 통해 이를 입증할 수 있는 세 가지 근거가 있습니다.

데이터 프라이버시

첫 번째, 데이터에 따르면 중견·중소 기업에 속하는 IT 의사 결정권자 중 90%가 데이터 프라이버시 프로그램을 숙지하고 있다고 답했습니다. 이는 대기업의 91%와 큰 차이가 없습니다.

그림 10. 조직의 데이터 프라이버시 프로그램을 대체로 숙지하고 있습니까? SMB N=481, 500+ N=2319.

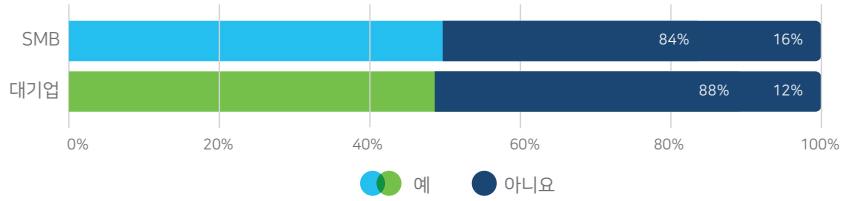


출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

사이버 보안 인식 교육

두 번째, 중견·중소 기업의 다수인 84%가 보안 인식 교육을 의무 사항으로 두고 있으며, 이는 대기업과 비교해 조금 낮은 수준입니다.

그림 11. 직원 사이버 보안 인식 교육이 조직 내 의무 사항입니까? SMB N=464, 500+ N=2272.

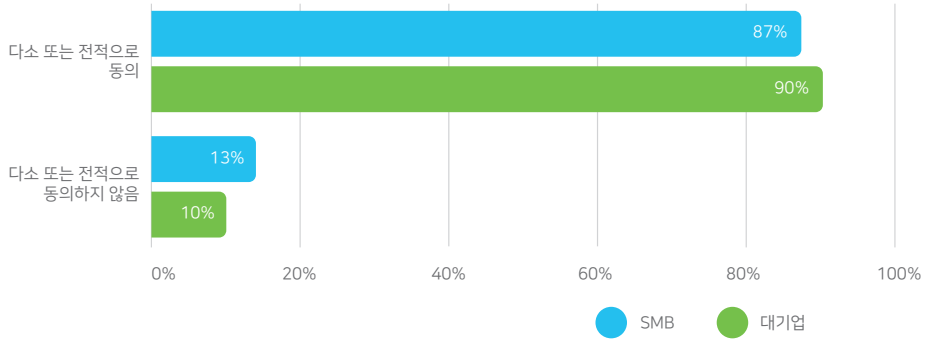


출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

임원진의 승인

세 번째, 중견·중소 기업 임원진의 87%가 보안이 우선순위가 높은 사항이라는 것에 동의합니다. 이는 대기업과 비교해 3% 낮은 수치입니다.

그림 12. 조직의 고위 임원진이 보안을 우선순위가 높은 사항이라고 생각합니까? SMB N=481, 500+ N=2319.

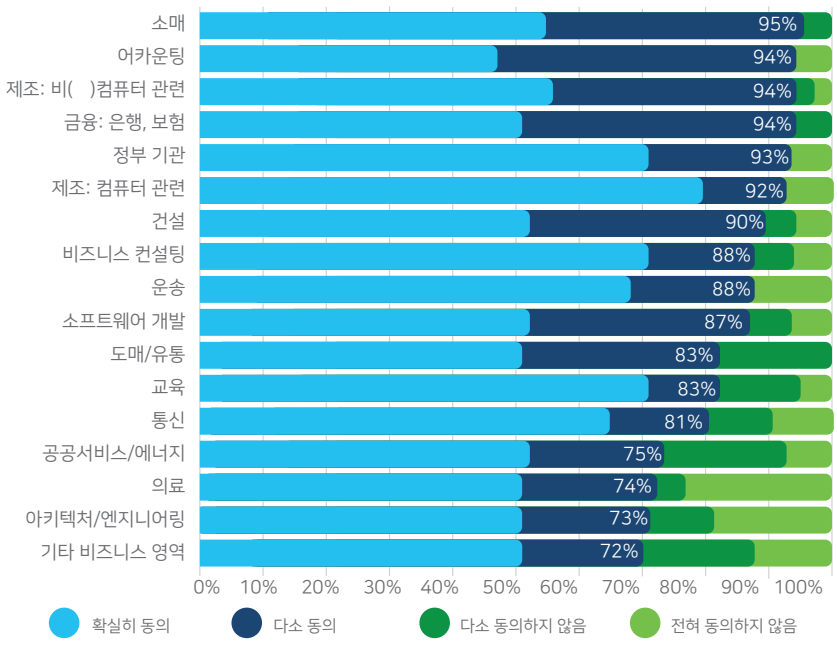


출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

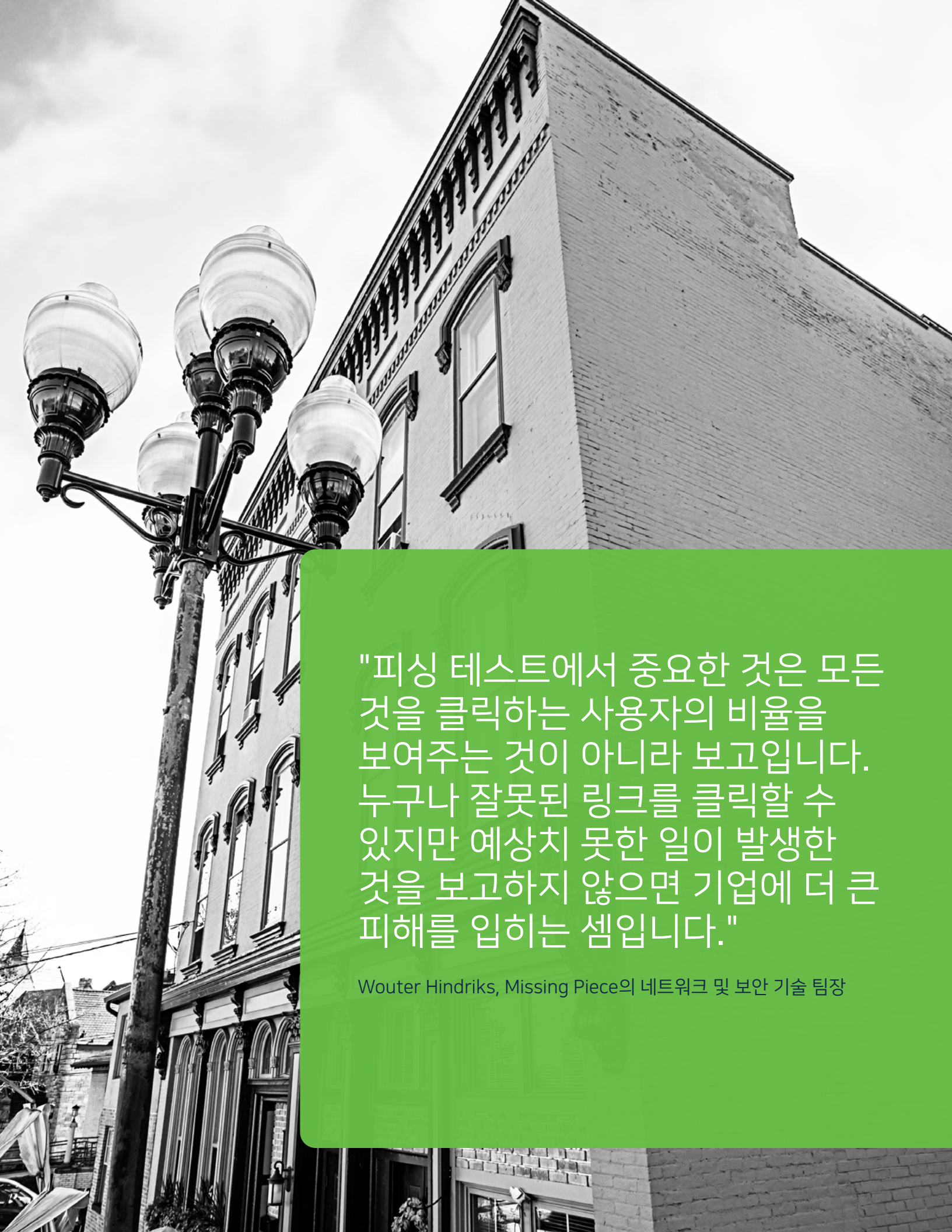
Cisco는 고객으로부터 비즈니스 전체적으로 보안이 도입되어야 그 효과가 발휘되고 보안 운용에 있어 임원진의 지원이 중요하다는 의견을 듣고 있으며, 이에 동의합니다. 대기업은 물론 중견·중소 기업에게도 이는 동일한 사실이며, 대부분의 경우 더욱 민첩한 환경에서 이를 달성하기 쉽습니다.

이상 세 가지 설문 조사 결과를 바탕으로 중견·중소 기업 역시 실제로 보안과 데이터 프라이버시에 관한 조직 문화가 성숙했음을 알았습니다. 모든 업계에 걸쳐 응답자의 2/3 이상이 임원진이 보안을 우선 사항으로 여기고 있다고 답했습니다(중견·중소 기업 답변만을 보여준 그림 13 참조).

그림 13. 조직의 고위 임원진이 보안을 우선순위가 높은 사항이라고 생각합니까? SMB N=481.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년



"피싱 테스트에서 중요한 것은 모든 것을 클릭하는 사용자의 비율을 보여주는 것이 아니라 보고입니다. 누구나 잘못된 링크를 클릭할 수 있지만 예상치 못한 일이 발생한 것을 보고하지 않으면 기업에 더 큰 피해를 입히는 셈입니다."

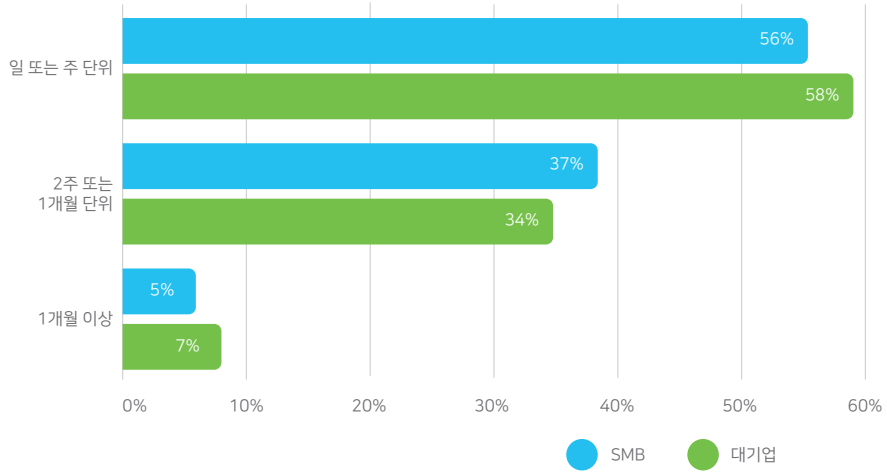
Wouter Hindriks, Missing Piece의 네트워크 및 보안 기술 팀장

통념 9: 규모가 작은 조직은 정기적으로 취약한 부분에 패치를 적용하지 않는다

패치를 적용하는 것은 사이버 보안의 기본인 경우가 많지만 실제로 이를 구현하기는 어려울 수 있습니다. 중견·중소 기업은 패치 적용으로 인해 발생하는 중단을 최소화하는 방법을 찾는 대신 다른 쪽에 리소스를 활용하고자 한다는 통념이 있습니다.

그렇지 않습니다. 중견·중소 기업의 56%가 일 또는 주 단위로 패치를 적용하며, 이는 대기업의 58%와 크게 차이가 나지 않습니다. 기업의 규모와 무관하게 패치 주기는 동일했습니다.

그림 14. 기업에서 소프트웨어의 드러난 취약점에 패치를 적용하는 주기가 어떻게 됩니까? SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

Cisco의 데이터에 따르면 직원 수가 500~999명인 기업 및 조직은 알려진 취약점으로 인한 사고를 경험할 가능성이 가장 높았습니다. 중견·중소 기업의 경우 대기업보다 알려진 취약점에 패치를 적용하는 것이 훨씬 효과적이었고, 그에 따라 사고의 수도 적었습니다.

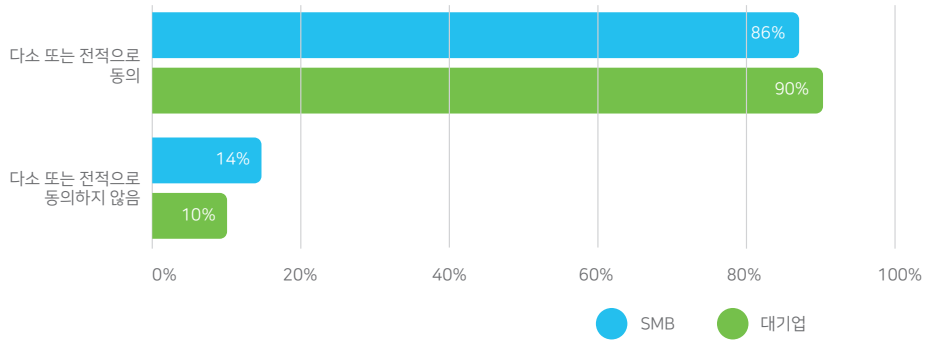
패치 적용은 미국 NIST SP 800-53 및 CIS(Center for Internet Security)에서 정의하는 것과 같이 최우선 방어 수단으로써 중요합니다. 중견·중소 기업이 이를 증명하고 있습니다.

통념 10: 중견·중소 기업은 보안 프로그램의 효율성을 측정할 수 없다

중견·중소 기업은 사이버 보안에 있어 '난사' 접근 방식을 채택한다고 추측하는 경우가 많습니다. 어떤 게 실제로 효과적인지 모니터링 및 측정할 수 있는 수단이 없고, 그에 따라 이를 최적화할 수 없다는 통념이 존재합니다.

그렇지 않습니다. 중견·중소 기업의 86%가 보안 프로그램의 효율성 평가를 위한 명확한 메트릭을 보유하고 있다고 답했습니다(대기업의 경우 90%).

그림 15. 조직의 임원진이 보안 프로그램의 효과를 평가하는 데 있어 분명한 메트릭을 마련했습니다. SMB N=481, 500+ N=2319.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

Cisco의 설문 조사 데이터에 따르면 조직의 규모와 무관하게 명확한 메트릭의 사용에는 차이가 거의 없었습니다. 이는 사이버 보안 제품이 지난 몇 년 동안 크게 발전했으며, 최고급 제품은 매우 분명한 지표를 제공할 수 있도록 설계되었습니다. 다시 말해 보고가 이전보다 더욱 쉬워졌습니다.

하지만 '측정할 수 없는 것은 수정할 수 없다'는 점에 있어서는 중견·중소 기업이 대기업에 미치지 못합니다. 응답자 가운데 46%가 임원진이 명확한 메트릭을 마련했다는 사실에 *전적으로 동의*했으며, 대기업의 경우 그 응답은 53%를 차지했습니다.

보안 최적화 기회 포착

중견·중소 기업이 강력한 보안을 실시하고 있다는 사실이 더욱 널리 알려져야 한다는 점이 입증되었지만 아직 개선해야 할 부분도 남아 있습니다. 현재의 벤더 환경에서 보안은 쉽게 바로잡을 수 없으며, 완전한 보안 역시 희망적이지만 비현실적입니다.

사이버 보안 피로

사이버 보안 피로는 악의적인 위협 행위자보다 앞서 행동하는 것을 포기하는 것으로 정의할 수 있으며, 놀랍게도 규모가 작은 기업 역시 대기업과 동일한 수준의 사이버 보안 피로를 겪고 있습니다. 중견·중소 기업 및 대기업 모두 응답자의 41%가 사이버 보안 피로를 경험하고 있다고 답했으며, 그렇지 않다는 답변은 58%였습니다. 더욱 효율적인 보안 관리가 이루어져야 하는 것이 분명합니다.

직원들의 사이버 보안 인식 채택

사용자가 사이버 보안 인식 프로그램을 채택하는 데 어려움을 겪은 중견·중소 기업 및 대기업은 보안 침해 다운타임에서 큰 차이를 보이지 않았습니다.

분명한 점은 사용자가 첫 번째 방어선일 수 있다는 점입니다. 하지만 사용자를 '가장 약한 연결 고리'로 여기는 것은 아닙니다. 그보다는 채택이 공통적으로 이루어지도록 사용자를 보안 전략에 포함시키는 것이 중요합니다.

보안의 민주화는 RSA 컨퍼런스 2020에서 Cisco의 CISO 자문 위원회 수장인 Wendy Nather가 발표한 기조 연설의 주제이기도 합니다. (Cisco 보안 사례 팟캐스트에서 Wendy와의 인터뷰를 들어볼 수 있습니다.)

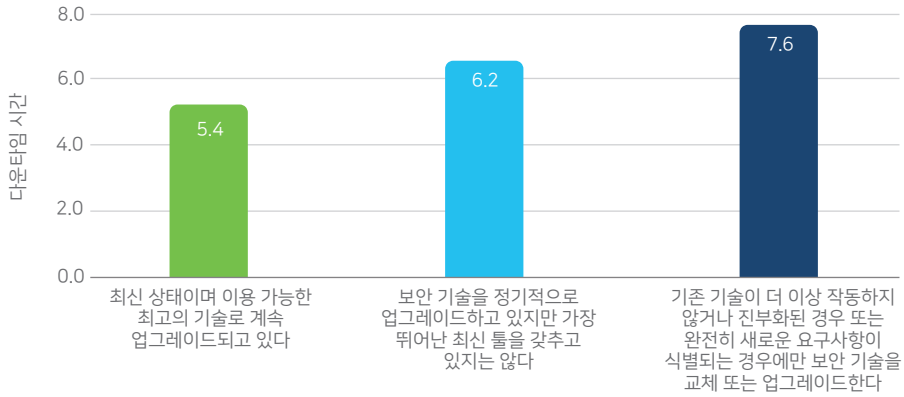
"시뮬레이션된 피싱 공격 중 하나에 당한 사용자를 비난하는 대신 이를 보고한 사용자를 응원하십시오. 모두에게 장려하고자 하는 행동을 측정하십시오."

Wendy Nather, Cisco CISO 자문 책임자

다운타임 감소

하드웨어와 소프트웨어가 오래될수록 새로운 위협을 막는 데 효율적이지 않다는 것이 사실일까요? Cisco의 데이터가 중견·중소 기업에 대한 이 가설의 근거가 되는 듯합니다.

그림 16. 지난 해에 가장 큰 영향을 미쳤던 보안 침해로 발생한 다운타임과 관련이 있는 조직의 보안 인프라를 어떻게 설명할 수 있습니까? SMB N=481.



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

더 이상 작동하지 않을 때가 되어서야 보안 기술을 교체 또는 업그레이드한다고 답한 중견·중소 기업 응답자는 지난 해 가장 심각한 보안 침해로 7.6시간의 다운타임을 경험했습니다. 최신 인프라를 보유한다고 답한 응답자는 5.4시간을 경험했다고 답했습니다.

그렇다면 모든 것을 버리고 가장 최신의 툴만을 구입해야 할까요? 전혀 그렇지 않습니다. 사이버 보안에 대한 Cisco의 경험에 따르면 노후 상태가 될 때까지 두는 대신 계속해서 작동하는 인프라 통합에 집중하고 필요에 따라 새로운 기술로 이를 보완하는 것이 더욱 중요합니다.

인프라가 오래되었다는 우려가 있는 경우 몇 가지 측면을 고려해 보십시오. 가장 중요한 것은 변화에 대처하는 유연성을 보장하는 것입니다. 정책 및 디바이스 관리를 지원하는 내장 자동화 및 분석을 제공하여 알려지지 않은 위협을 탐지하고 대응 및 정책 변화를 조정하는 것이 이상적입니다.

플랫폼에서 분석을 적용하여 온프레미스 및 클라우드 네트워크 트래픽에서 이상 행동을 파악할 수 있는지 확인하십시오. 정책을 시행하고 침해를 당한 엔드포인트에 대한 네트워크 및 애플리케이션 액세스를 자동으로 채택하면서 이를 수행할 수 있어야 합니다.

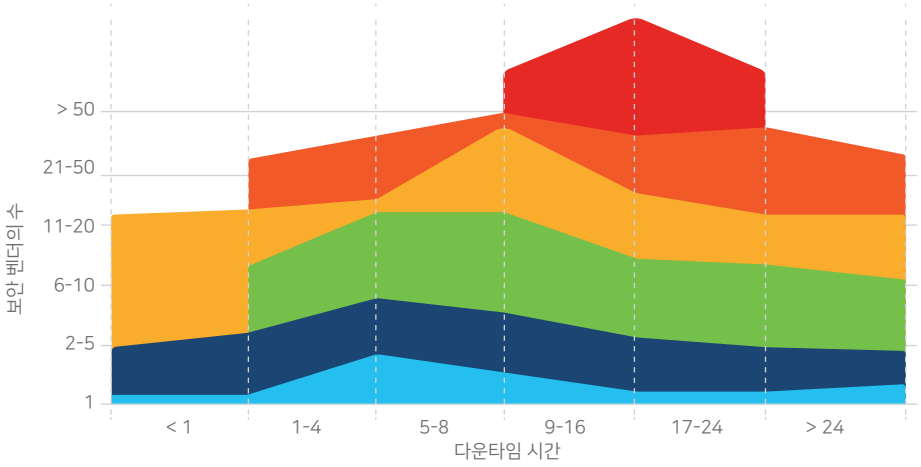
자세히 알아보려면 보안 플랫폼 벤더에게 묻는 5가지 질문을 읽어보십시오.

벤더 복잡성

많은 조직에 있어 벤더 증가가 보안 위험 확산을 의미할 수도 있습니다. 이러한 접근 방식의 결과는 무엇입니까? 멀티 벤더 환경을 관리하는 것이 얼마나 어려운 일이며, 더 많은 벤더를 확보하는 것이 다운타임 감소를 통해 보안 개선이라는 결과로 이어질까요?

놀랍게도 중견·중소 기업 응답자들은 벤더의 수가 많을수록 가장 심각한 보안 침해로 인해 다운타임이 더 길었다고 답했습니다. 벤더가 1개인 기업의 경우 다운타임이 평균 4시간인 것에 비해 벤더 수가 50개 이상인 기업은 4배 이상인 17시간을 초과했습니다.

그림 17. 보안 환경 내에서 활용하는 보안 벤더의 수[SMB N=472]와 지난 1년 동안 발생한 가장 심각한 보안 침해로 인해 발생한 시스템 다운타임[SMB N = 388].



출처: Cisco - 소규모 비즈니스 세계의 큰 보안 보고서, 2020년

그림 17에서 알 수 있듯 벤더의 수가 많을수록(아래에서 위 순서) 다운타임이 길어집니다 (왼쪽에서 오른쪽 순서). 일반적인 중견·중소 기업 보안 환경에서 벤더는 불필요한 복잡성과 비효율적인 워크플로를 유발할 수 있으며, 시스템 다운타임 측면에서 비즈니스의 성패를 좌우할 수 있습니다.

멀티 벤더 환경으로 인해 발생하는 복잡성 문제를 완화하는 훌륭한 전략은 솔루션을 함께 사용할 수 있는 개방형 포트폴리오 기반 플랫폼을 도입하는 것입니다.

발전을 보장하는 리소스

요약하자면, Cisco의 데이터는 중견·중소 기업이 전략적 계획 및 일상 업무에서 보안을 심각하게 고려하고 있음을 보여줍니다. 아주 좋은 소식입니다!

하지만 Cisco의 2020 CISO 벤치마크 연구에 따르면, 새로운 보안 당면 과제는 매일 새롭게 발생하고 있습니다.

중견·중소 기업의 경우 이를 따라잡고 비즈니스를 성장시켜야 한다는 압박이 커지고 있습니다. 여기에 모바일 및 원격 인력의 증가는 더 큰 압박입니다.

이 여정에 도움이 되도록 중견·중소 기업 전용 웹 사이트인 중견·중소 기업 보안 솔루션에 방문해 보십시오. 사이버 보안을 통해 성공을 가속화하는 데 도움이 될 몇 가지 리소스가 있습니다.

- The End of the Password... Finally
- Cloud Security for the Future of Your Business
- Small Business Product Selector
- 3 Tips for Choosing a Next-Generation Firewall for Small Business
- Cisco 중견·중소 기업 보안 고객 사례 연구

Cisco는 보안 솔루션이 팀으로 작동하면서 서로 학습, 청취 및 대응해야 한다는 아이디어를 토대로 보안 플랫폼을 구축했습니다. 이것이 보안을 간소화하고 효율성을 높이는 체계적 접근 방식이라고 생각합니다.

Cisco SecureX는 기존 인프라를 통합하여 일관된 환경을 제공합니다. 가시성을 통합하고, 자동화를 지원하며, 네트워크, 엔드포인트, 클라우드, 애플리케이션 전반에 걸쳐 보안을 강화 합니다.

원격 인력 보안 확보

원격 인력을 대규모로 지원하는 방향으로 급작스럽게 전환한다면 그에 따라 보안 당면 과제가 발생합니다. 조직이 그 이전과는 다른 환경에서 움직여야 하기 때문입니다. 이는 보안 침해를 발생시키지 않으면서 전례가 없는 수의 원격 인력과 이들의 디바이스에 지원을 제공해야 하는 보안 및 IT 팀 모두에게 갑작스러운 부담이 됩니다.

더 많은 원격 작업에 적응해야 하는 중견·중소 기업의 경우 어떻게 보안을 유지해야 합니까? 이 새로운 현실을 고려하여, 비즈니스의 속도와 규모에 따라 원격 인력을 보호하는 간단하고 쉬운 방법이 필요합니다.

Cisco는 직원이 원격 상태에서 안전하게 업무를 수행할 수 있도록 지원하고자 합니다. 다음 단계를 권장합니다.

첫 번째, 기본을 숙지하십시오. 이 보고서에서 논의한 기본 사항으로는 취약점 패치 적용, 직원 교육, MFA(Multi-Factor Authentication)를 통한 제로 트러스트 액세스 구현, 네트워크, 엔드포인트, 클라우드 및 애플리케이션 보안이 있습니다.

두 번째, 사용 편의성과 보안의 균형을 조정하십시오. 직원들이 보안 전문가가 되어 그들이 아는 것을 모두 알 필요는 없습니다. 직원은 각자의 업무를 수행해야 합니다. 원활한 업무가 가능하도록 액세스 가능한 보안이 이루어져야 합니다.

세 번째, 보안 벤더와 파트너십을 이루십시오. 단, 이 보안 벤더는 보안 인프라의 간소화에 도움이 되어야 하지, 이를 더욱 복잡하게 만들어서는 안 됩니다. Cisco의 데이터에 따르면 벤더의 수가 적을수록(그리고 더욱 전략적일수록) 보안 침해로 인한 다운타임이 감소합니다.

조직의 보안을 유지하는 데 유용한 기사, 웹 세미나 및 오퍼는 Cisco Secure Remote Worker를 방문해서 알아보십시오.

Cisco 전문가 소개

CISO 자문 위원회는 Cisco 보안 소속으로 다양한 분야의 경험과 사이버 보안 지식을 보유한 CISO 출신 위원으로 구성되어 있습니다. 사이버 보안 보고서 시리즈에서 제공하는 권장 사항에 대한 인사이트, 안내 및 경험을 제공하는 것 외에도 셀러, 파트너 및 고객의 규정 준수, 프라이버시, 모니터링 및 가시성, 제로 트러스트 및 위협 인텔리전스에 관한 디지털 혁신을 지원합니다. CISO 자문 팀과 상담하려면 asktheciso@external.cisco.com으로 문의하십시오.

Cisco 사이버 보안 보고서 시리즈 소개

지난 10년간 Cisco Talos는 전 세계 사이버 보안 현황에 관심 있는 보안 전문가들을 위해 수많은 최종적 보안 및 위협 분석 정보 보고서를 발간했습니다. 이 종합 보고서들은 업계의 보안 위협 현황과 그것이 기업에 미치는 영향을 비롯해 데이터 유출로 인한 피해를 막을 수 있는 모범 사례에 대해 자세히 설명하고 있습니다.

Cisco 보안에서는 Cisco 사이버 보안 시리즈를 통해 연구 및 데이터 기반 출간물을 내놓습니다. Cisco Talos는 관심사가 각기 다른 보안 전문가들의 기대에 부응하고자 보고서의 주제와 내용을 다각화하기로 결정했습니다다. 보안 업계의 위협 연구 및 혁신 전문자들의 심층적이고 폭넓은 전문성을 바탕으로 하는 사이버 보안 시리즈에는 데이터 프라이버시 벤치마크 조사, 위협 보고서, CISO 벤치마크 연구, 그리고 기타 연중 발간된 보고서가 포함됩니다.

자세한 내용을 확인하고 모든 보고서와 보관 사본에 액세스하려면 www.cisco.com/go/securityreports를 방문하십시오.

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, 네덜란드

Cisco has more than 200 offices worldwide. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 www.cisco.com/go/offices에서 확인하십시오.

2020년 5월 출간 SMB_05_2020

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco 및 Cisco 로고는 미국과 기타 국가에서 Cisco 및 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 URL www.cisco.com/go/trademarks를 참조하십시오. 언급된 타사 상표는 해당 소유권자의 재산입니다. '파트너'라는 용어의 사용이 Cisco와 다른 회사 간의 파트너십 관계를 의미하는 것은 아닙니다. (2059788)

cisco Secure


cisco Secure