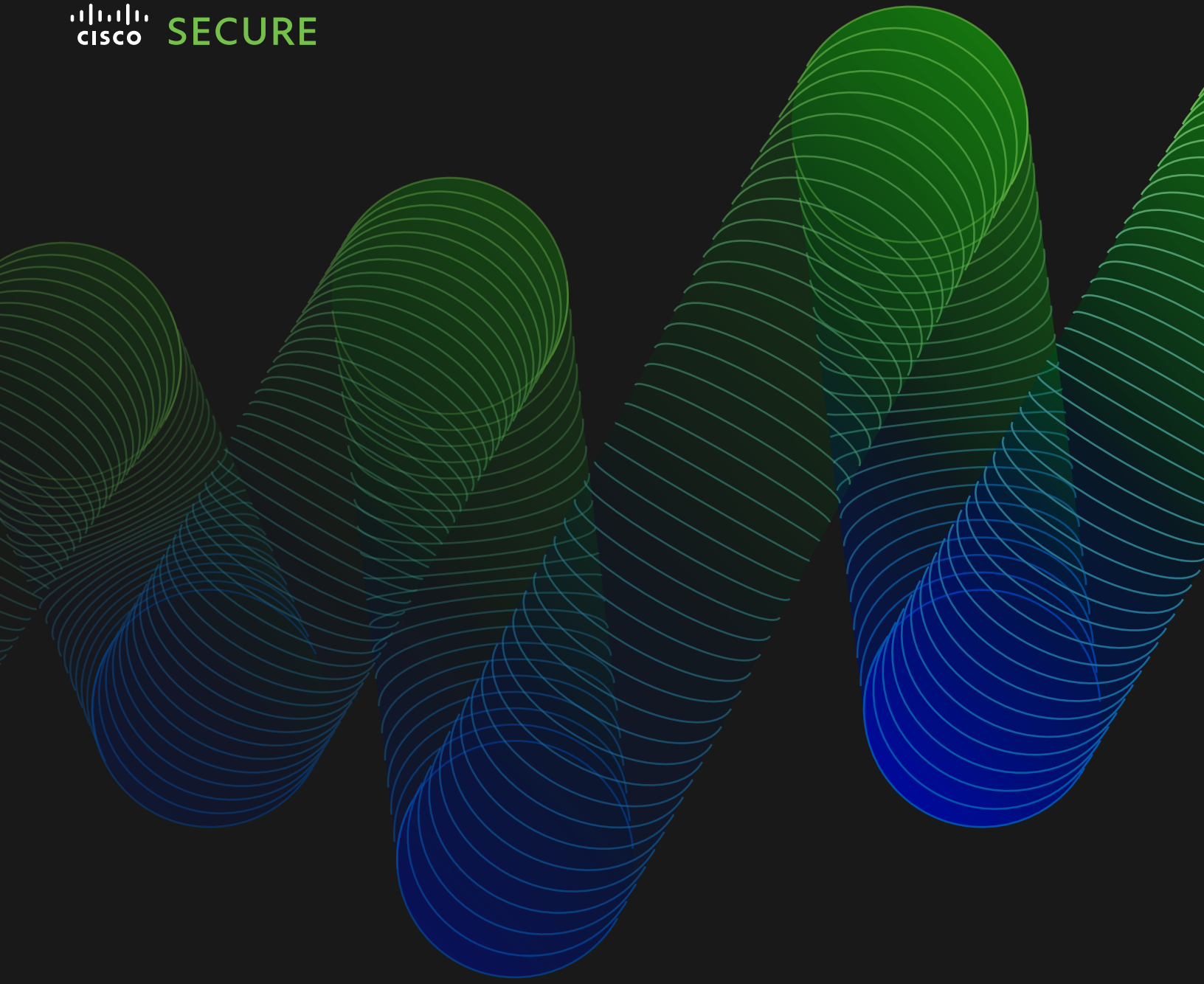
cisco SECURE



보안성과연구

3권

보안 탄력성 확보

목차

서문

탄력성이라는 단어를 생각하면 무엇이 떠오르나요? 저는 (셰익스피어의 표현을 빌리자면) " 가혹한 운명의 돌팔매와 화살" 에도 불구하고 더욱 강해질 용기와 대담함을 가진 사람이나 무언가를 떠올리실 것이라 생각합니다.

이는 완벽하게 만족스러운 정의이며 저는 그 정신에 박수를 보냅니다. 그러나 대기업과 중소기업의 보안에 관한 경우, 보안이 손상된 후에 회복할 수 있을 만큼의 탄력성은 부족할 수도 있습니다. 랜섬웨어나 지적재산권 도용과 같은 사이버 보안 침해는 기업, 직원, 파트너, 심지어 고객에게도 큰 피해를 줄 수 있기 때문입니다. 2021년 보안성과연구에서 조사 대상 기업 중 41%가 최근 2년 이내에 중대한 보안 사고나 손실을 경험했다고 답한 것을 보면 이 문제가 얼마나 광범위하게 퍼져 있는지 알 수 있습니다.

시스코에서 정의하는 보안 탄력성이란 단순한 생존이 아니라 기업이 예측할 수 없는 위협이나 변화를 극복하고 더욱 강력하게 성장할 수 있도록 모든 측면의 무결성을 보호할 수 있는 능력입니다. 시스코 보안성과연구 3권에서 알 수 있듯이, 설문조사에 참여한 임원진들은 보안 탄력성 달성이 비즈니스에 매우 중요하다는 데 거의 만장일치로 동의했습니다. 오늘날 더 많은 기업들이 상호 연결됨에 따라 가치 사슬(value chain)의 누군가에 대한 침해가 다른 사람들에게 극적인 파급 효과를 미칠 수 있다는 것은 놀라운 일이 아닙니다. **제 역할을 다하지 않았다고 알려지길 원하는 임원은 아무도 없습니다.**

그러니 이 보고서를 즐겁게 활용하시길 바랍니다. 원하는 수준의 보안 탄력성을 달성하기 위한 전략을 수립하고 솔루션 개발에 유용한 자료가 되기를 바랍니다. 위협에 대한 탄력성. 변화에 대한 탄력성. 미지의 것에 대한 탄력성. 보안 업계에서는 유행어가 넘쳐나고 있습니다. 하지만 탄력성이라는 단어는 한동안 계속 남아있을 것 같습니다. 아마도 위대한 셰익스피어의 희곡인 *햄릿*만큼 길지는 않겠지만 그래도 꽤 긴 시간 사용될 것입니다.

— **Shailaja Shankar**
Cisco Secure SVP 겸 GM

출처: 시스코 '2021 보안성과연구: 엔드포인트 에디션'

"세상은 고통으로 가득하지만,
이에 대한 극복으로도
가득합니다."

— 헬렌 켈러

소개

보안은 결코 쉽지 않습니다. 그러나 지난 몇 년 동안 사이버 사고로부터 기업을 보호해야 하는 상황은 더욱 심화되었습니다. 오늘날의 보안 방어자들은 증가하는 위협과 확대되는 공격 표면뿐 아니라 전쟁, 기후 변화, 금융 불안정 그리고 물론 글로벌 팬데믹 같은 더 큰 상황도 고려해야 합니다.

이러한 격동의 환경에서 탄력성이라는 개념은 대부분의 기업 아젠다에서 가장 중요한 요소가 되었습니다. **기업이 이렇게 빠르고 획기적인 변화에 신속하게 적응하고 더욱 강해지려면 어떻게 해야 할까요?**

이번 보안성과연구 3권에서는 보안 탄력성을 이해하기 쉽게 설명하고 실행 가능한 통찰력을 제공합니다. (왜냐하면 귀하는 다른 일로 바쁘실 것이기 때문입니다.) 어떤 보고서도 이 거대한 주제에 대해 빠짐없이 다룰 수는 없지만, 여기에서는 향후 사이버 보안 전략을 구축하고 개선하실 때 고려해야 할 몇 가지 주요 사항을 다루었습니다.

26개국 4,700명 이상의 보안 전문가로부터 수집한 데이터를 통해 사이버 탄력성을 강화할 **7가지 성공 요인**을 발견했습니다. 또한 이 보고서에서는 보안 탄력성의 의미, 보안 탄력성이 중요한 이유, 기업이 생각하는 자체 탄력성 순위를 정확하게 분석합니다.

미래에 어떤 일이 발생하더라도 번창할 수 있도록 조직을 구성하실 때 데이터가 자원으로 사용되고 더 많은 확신을 제공해 드리길 바랍니다.

위험과 탄력성 사이에는 다리가 있습니다. 때로는 그 여정이 힘들다는 것을 알고 있으므로 시스코가 도와드리겠습니다.

주요 조사 결과

임원진들은 보안 탄력성을 가장 중요하게 여기며, **96%**는 그중 비즈니스에 **매우 중요**하다고 생각합니다.

조직의 **2/3**가 비즈니스 운영을 위태롭게 하는 **주요 보안 사고를 경험**한 적이 있다고 했습니다.

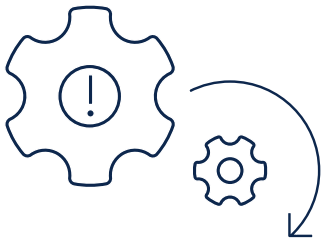
문화가 중요합니다.

보안 문화를 조성하는 조직은 탄력성이 46% 향상되었습니다.

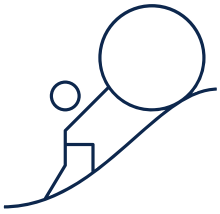
아키텍처가 중요합니다.

성숙한 Zero Trust, XDR, SASE를 구현한 조직은 모두 상당히 높은 탄력성 점수를 자랑합니다.

최우선순위



보안 탄력성 전반에서 최고의 우선순위 두 가지는 **사고 방지** 및 **손실 완화**입니다.



보안 인재를 유지하는 것은 탄력성 우선순위는 가장 낮지만 모든 유형의 조직에서 **가장 어려운** 과제이기도 합니다.

최저 우선순위

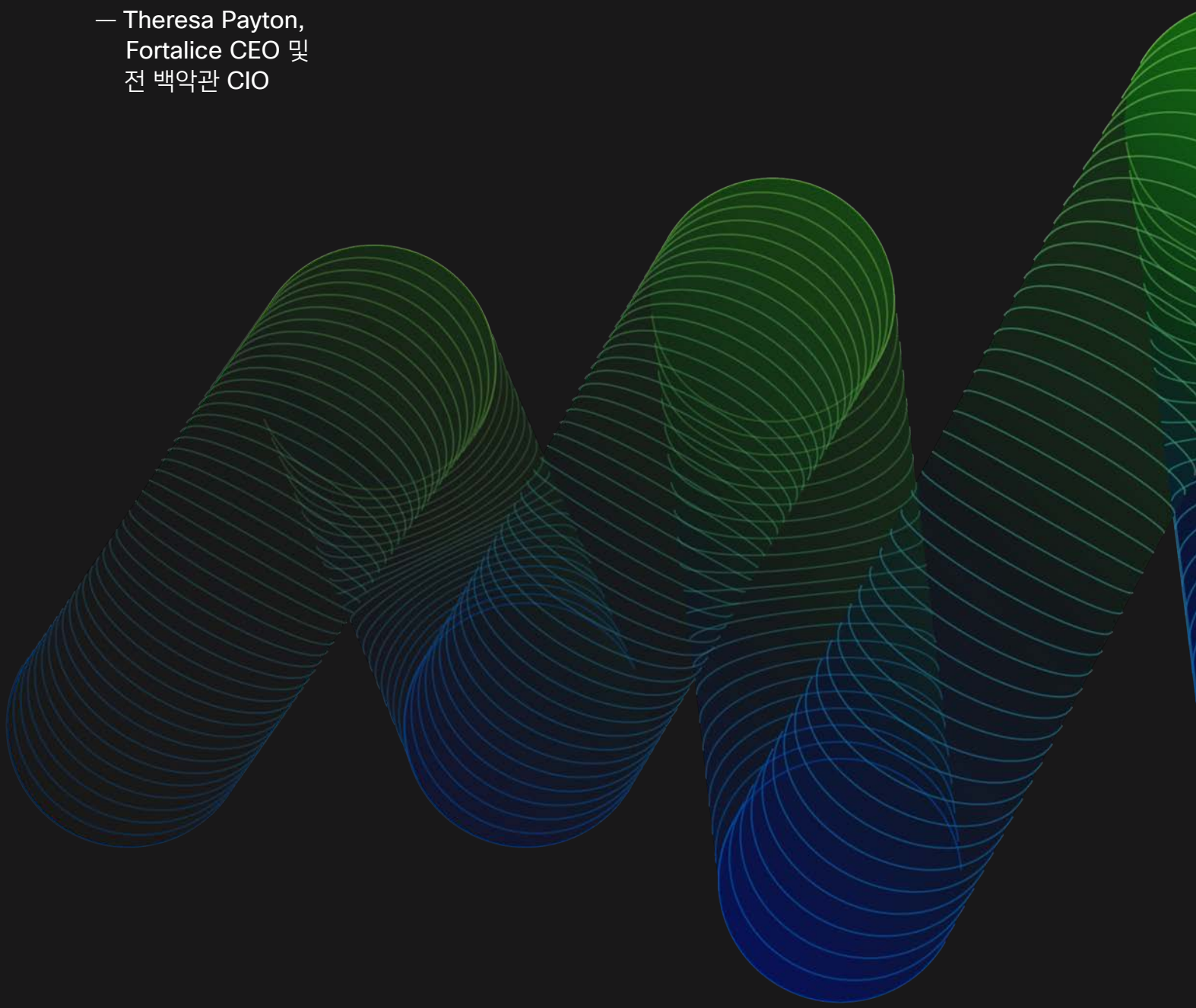
성공 요인 7가지를 확인했으며, 이 요인이 달성될 경우 하위 10 백분위수에서 상위 10 백분위수로 전체 **보안 탄력성** 조치가 **강화**됩니다.

설문 조사 정보

샘플링 방법	시스코는 전문 설문조사 연구 기관에 의뢰하여 계층화된 무작위 샘플링 기법으로 2022년 중반에 완전한 익명 설문조사를 실시했습니다.
설문조사 참가자	26개국의 현직 IT, 보안 및 프라이버시 전문가 4,751명 이상을 대상으로 설문조사를 실시했습니다. 샘플 인구 통계는 부록을 참조하십시오.
데이터 분석	Cyentia Institute에서 시스코 대신 설문조사 데이터를 독립적으로 분석하여 본 보고서에 소개된 모든 결과를 도출했습니다.

"보안성과연구의 신중한 접근 방식이 인상적이었습니다. 자원을 가장 잘 활용하여 보안 프로그램의 영향을 극대화하는 방법에 대한 데이터 기반 지침을 제공하고 있습니다."

— Theresa Payton,
Fortalice CEO 및
전 백악관 CIO



보안 탄력성이란?

" 탄력성" 이 유행어라고 생각하시든 아니라고 생각하시든, 사이버 보안 분야 안팎의 많은 이들의 생각과 말에 자리잡고 있다는 것은 부인할 수 없는 사실입니다. 하지만 그 의미는 정확히 무엇일까요? 이 주제에 대해서는 시스코 나름의 의견이 있지만 이 보고서는 4,700명 이상의 보안 전문가를 대상으로 한 설문조사이므로 그들의 의견을 대신 전하겠습니다.

"그 단어를 계속 사용하고 계신데 저는 그 단어의 의미가 당신이 생각하는 그 뜻이라고 생각하지 않아요."

— 이니고 몬토야, 영화 *프린세스 브라이드*

조직에서 보안(또는 사이버) 탄력성의 의미를 설명해 달라는 질문에 응답자들은 광범위한 답변을 했습니다. 하지만 그중 몇 가지 주제가 공통적으로 나타나는 것을 확인했습니다.

" 견딤(withstand)" , " 회복(recover)" , " 예상(anticipate)" , " 적응(anticipate)" , " 불리(adverse)" 등의 단어가 모두 응답자들이 생각하는 핵심적인 보안 탄력성 개념으로 나타납니다. 이러한 단어가 이상하게도 친숙하다면, 아마 NIST의 사이버 탄력성에 대한 정의에서 거의 나왔기 때문일 것입니다. 이는 전혀 문제될 것이 없고, 이런 설문조사에서 부정행위는 하지 않습니다. 그러나 탄력성의 의미가 불분명하여 다수의 보안 전문가조차 무슨 뜻인지 찾아봐야 한다는 점을 시사합니다. 다음 섹션에서는 해당 개념을 더 명확하게 정리해 보겠습니다.

사이버 탄력성:

사이버 자원을 사용하거나 사이버 자원의 지원을 받는 시스템에서 불리한 조건, 스트레스, 공격, 손상을 예측하고, 견디며, 해당 상황 후에 복구하고, 해당 상황에 적응할 수 있는 능력입니다.

— 출처: NIST SP 800-172

보안 탄력성이 중요한 이유

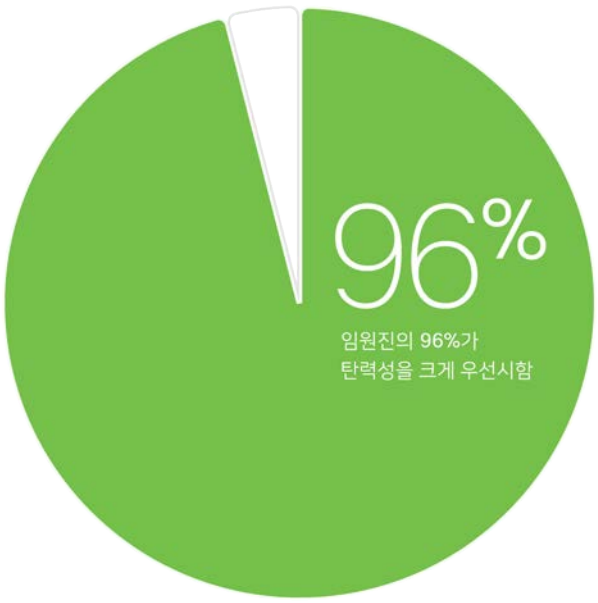
반대 의견이 있는 이들은 이 섹션 제목을 읽고 " 그것이 대단한 문제라는 확신이 들지 않는다" 고 생각할 수 있습니다." 그럴 수 있습니다. 우리의 의견은 공허한 주장이 아니므로 처음부터 근거를 제시해 보겠습니다.

우리는 응답자들에게 조직의 최고위 임원진이 보안 탄력성에 대해 얼마나 관심이 있고 중요하게 생각하는지 물었습니다. 그 메시지는 아주 분명했습니다. **임원진 중 96%가 보안 탄력성을 매우 중요하게 생각합니다.** 그것이 바로 보안 탄력성이 대단히 중요하다는 근거가 된다고 생각합니다.

임원진들이 보안 탄력성에 높은 우선순위를 두는 것은 많은 사람들이 그 위험을 잘 알고 있다는 사실에서 비롯되었을 것입니다. **응답자의 약 2/3가 비즈니스 운영을 위태롭게 하는 주요 보안 사고를 경험한 적이 있다고 했습니다.**

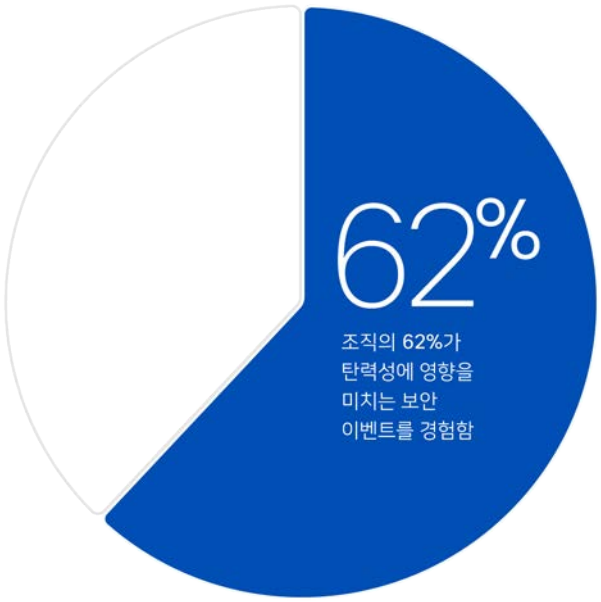
또한 해당 보안 사고 중 대부분은 지난 2년 이내에 발생했다고 합니다. 이를 통해 보안 탄력성이 선구자적 사상가나 임원진들의 마음 속에서만 중요한 것이 아니라고 추론하게 됩니다. 이는 전 세계 대부분의 조직에서 매우 중요한 개념입니다.

그림 1: 임원진들은 보안 탄력성에 얼마나 관심이 있고 얼마나 중요하게 생각합니까?



출처: 시스코 보안성과연구

그림 2: 조직에서 탄력성에 영향을 미치는 보안 사고를 경험한 적이 있습니까?

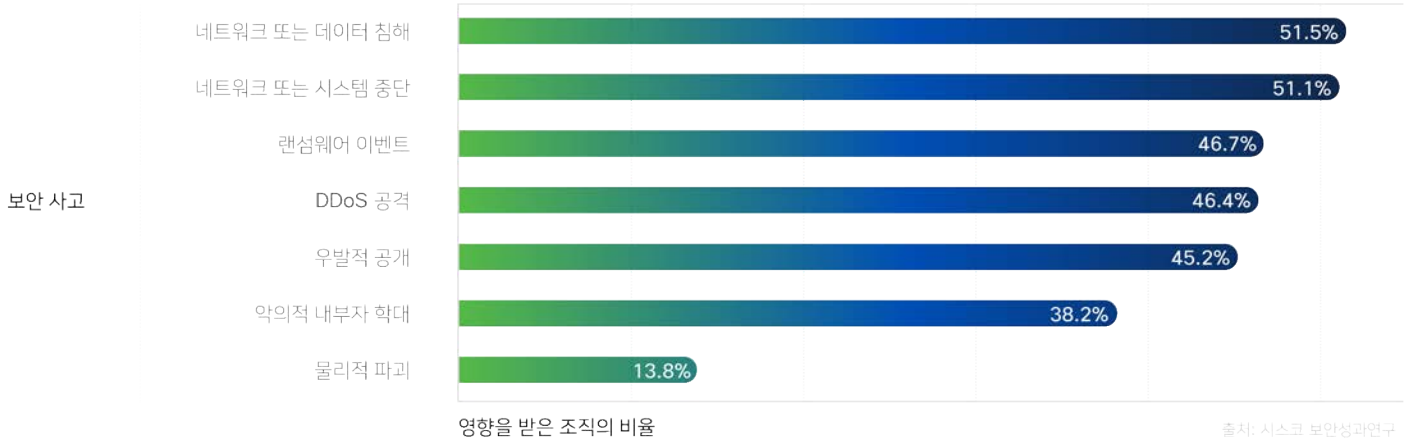


출처: 시스코 보안성과연구

그런 다음 응답자들에게 그들이 경험했던 탄력성에 영향을 미치는 사고의 유형을 자세히 설명해 달라고 요청했습니다. 그림 3에서 볼 수 있듯이, 이전에 사고를 겪었다는 참가자의 절반 이상이 네트워크/데이터 침해와 네트워크/시스템 중단을 언급했습니다. 랜섬웨어 공격과 DDoS(Distributed Denial-of-Service) 공격은 그 다음으로 흔한 이벤트 유형으로, 각각 약 46%의 조직에 영향을 미칩니다.

앞서 언급한 사고 유형에서는 직원을 공격(예: 피싱 이메일 클릭)의 벡터로 거의 확실하게 포함하는 경우도 있었지만, 내부자에 의한 악의적인 오용을 경험한 조직은 약 38%였습니다. 물리적 파괴 행위와 방해 행위도 언급되었지만, 다른 사고 유형보다는 빈도가 훨씬 낮았습니다.

그림 3: 탄력성에 영향을 미치는 보안 사고 유형

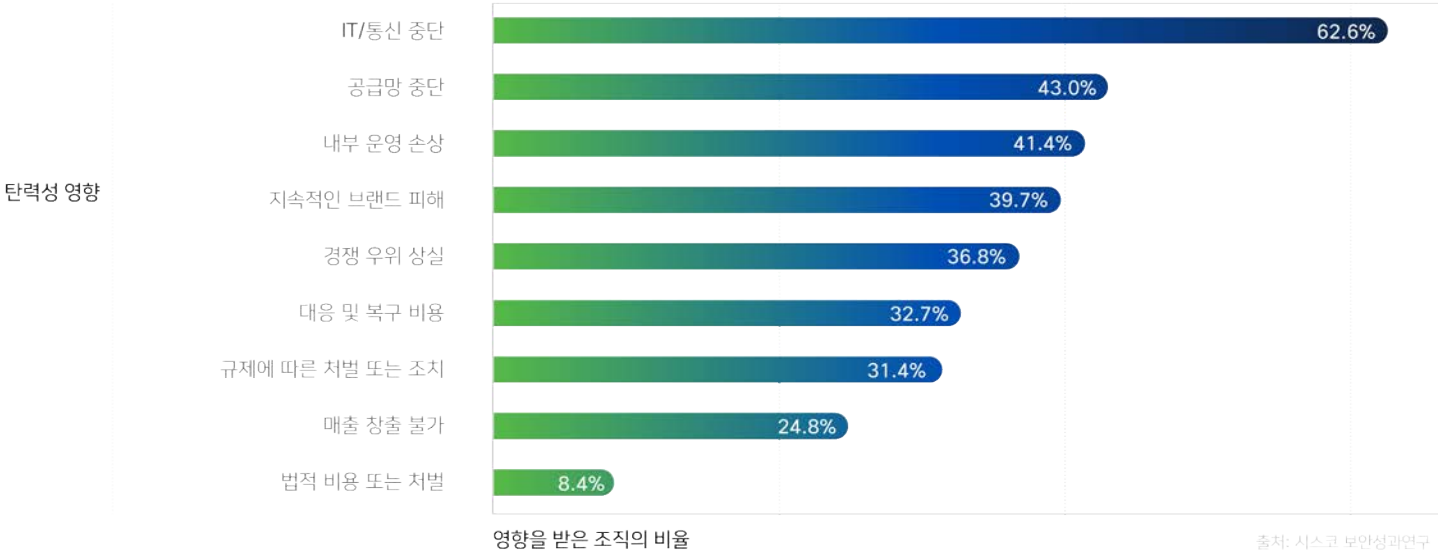


출처: 시스코 보안성과연구

또한 이러한 이벤트가 조직에 어떤 영향을 미치는지에 대한 응답자들의 의견은 다양했습니다(그림 4 참조). 60% 이상이 IT와 통신 장애 및 보안 탄력성과 관련한 ICT 역할이 중요함을 언급했습니다. 비즈니스 수준에 미치는 영향에서 공급망 중단은 2위를 차지했습니다. 그런 고통은 최근 들어 우리 모두 겪고 있으므로 조직도 느낀다는 것은 놀랄 일이 아닙니다.

공급망 운영에 미치는 영향은 피해를 입은 조직의 외부 기관에도 영향을 미치지만 (약 41%의 기업이 겪었다고 보고된) 내부 운영 중단은 내부에 큰 피해를 입힙니다. 브랜드 피해는 많은 임원진이 " 계속해서 밤을 지새우는 이유" 목록의 상단에 위치하므로, 이러한 사고의 약 40%로 인해 해당 결과가 발생한다는 것을 알 수 있습니다. 경쟁 우위 상실은 또 다른 주요 우려 사항으로, 이는 상위 5개 탄력성 영향을 마무리합니다.

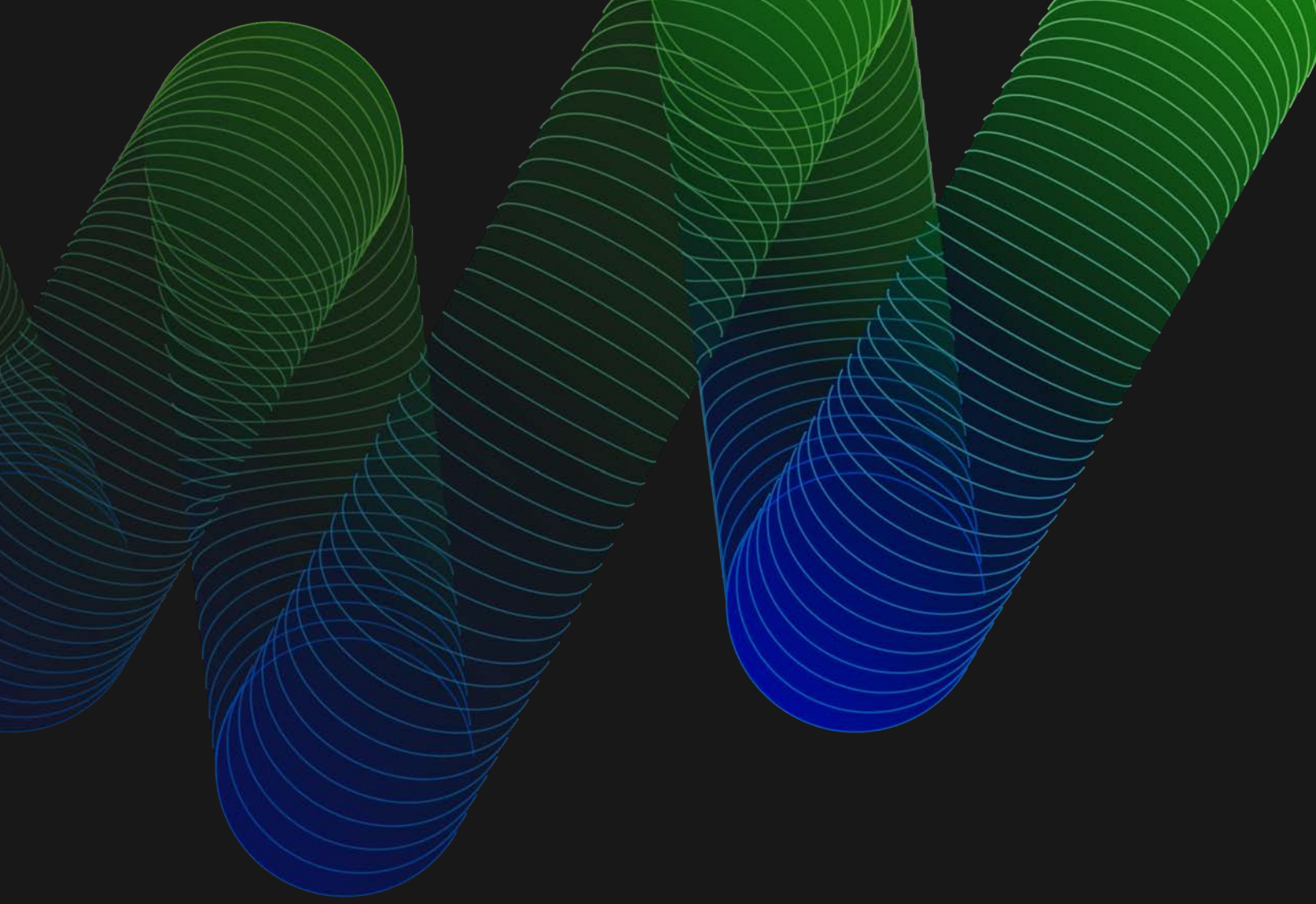
그림 4: 보안 사고로 인한 탄력성 영향의 유형



출처: 시스코 보안성과연구

조직이 이러한 사건을 방지하고 보안 탄력성을 향상하려면 어떻게 해야 합니까? 그것이 이 보고서에서 답하고자 하는 주요 질문 중 하나입니다. 처음부터 다른 무엇보다 한 가지 일을 하고 있다는 것은 분명한데, 그것은 바로 돈을 쓰는 것입니다. 놀랍게도 최근에 주요 사고 발생 후에 조직이 보안에 대한 투자를 늘렸다는 참가자가 96%에 달했습니다.

이제, 우리 모두는 돈을 쓰는 것만으로 문제가 해결하지 못한다는 것을 알고 있습니다. 하지만 해결책을 무료로 얻을 수 없다는 것도 압니다. 중요한 것은 어떤 투자를 했을 때 수익을 얻고 어떤 투자를 했을 때 그렇지 않은가 하는 질문입니다. 우리가 얻은 교훈은 조금 후에 알려드리겠습니다. 그러나 그 전에 보안 탄력성이라는 범주 아래의 주요 목표를 살펴보겠습니다.



"결국 보안은 위험한 비즈니스입니다. 우리는 모든 곳에서 모든 것을 보호하지는 않습니다. 그러지 않으면 비즈니스가 이루어지지 않을 것이기 때문입니다. 그러나 보안 탄력성을 통해 조직에 가장 많은 가치를 부여하는 비즈니스 부문에 보안 자원을 집중하고 가치를 보호할 수 있습니다."

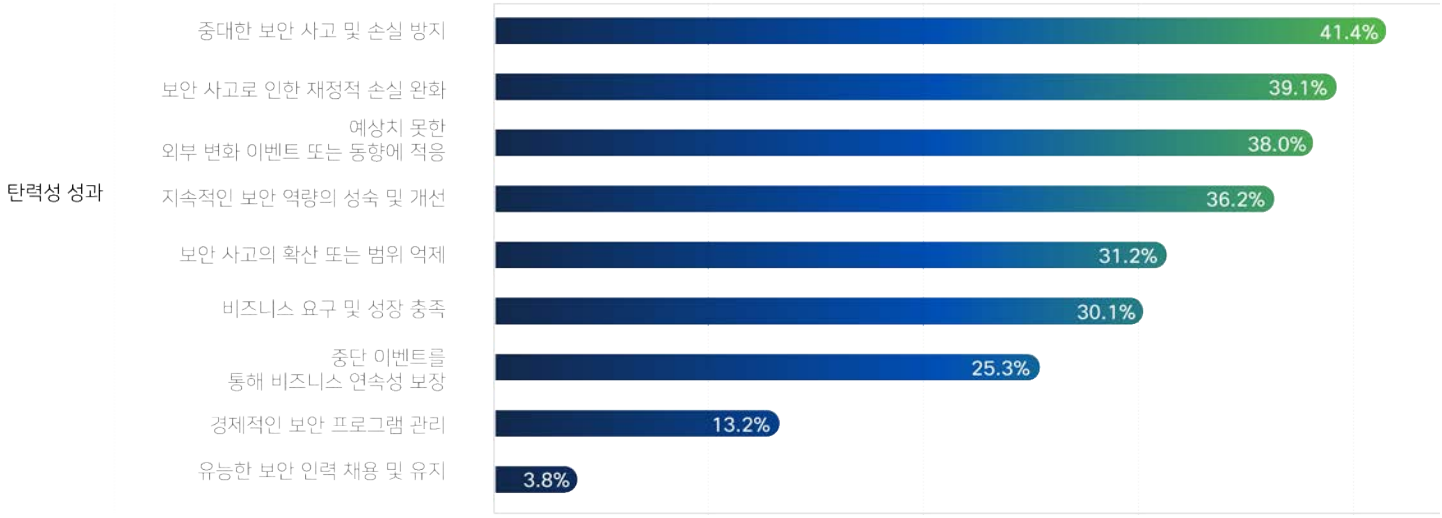
— Helen Patton,
Cisco Security Business Group의 CISO

보안 탄력성에 수반되는 사항은 무엇입니까?

마지막 섹션을 통해 우리는 보안 탄력성이 임원진들에게 중요한 문제라는 것을 알게 되었지만 실제로 보안 탄력성에 수반되는 사항은 무엇입니까? 조직에 탄력성이 있을 때 특징이나 성과는 무엇입니까? 이 설문조사를 준비하기 위해 보안 리더들에게 보안 탄력성에 대한 목표를 물어보았습니다. 그런 다음 그들의 응답을 검토하고 9가지 주요 보안 탄력성 성과로 분류했습니다.

현재의 글로벌 설문조사로 돌아가 참가자들에게 조직에서 가장 중요하게 생각하는 9가지 주요 탄력성 성과는 무엇인지 질문했습니다(최대 3가지 선택 가능). 그림 5는 해당 응답을 전체적으로 보여줍니다.

그림 5: 참가자들이 가장 중요하다고 선택한 보안 탄력성 성과



출처: 시스코 보안성과연구

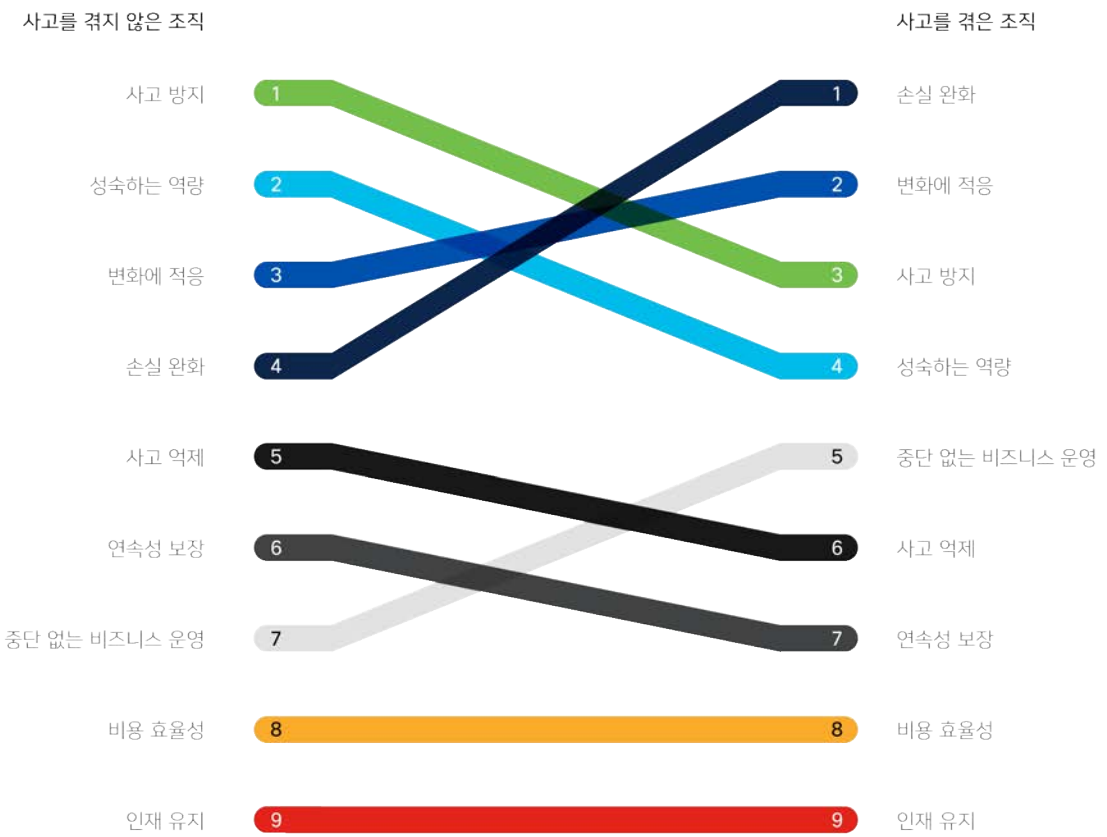
만장일치로 탄력성을 " 공격에 대한 즉각적인 반응" 으로 여기는 중에 사고 예방이 1위로 선정되어 다소 놀랍습니다. 그러나 재정 손실 완화와 더불어 1위 및 2위의 타겟은 위험에 대한 고전적인 정의인 확률 및 영향입니다.

그 다음은 예상치 못한 사고에 대한 적응으로, 앞서 공유한 주관식 응답에서 설명한 주제로 되돌아갑니다. 코로나19 팬데믹과 관련된 최근 경험 때문에 이 항목이 목록에 올라가게 되었는지 의문을 품을 수밖에 없습니다.

9가지 성과에 대해 모두 언급하지는 않고, 마지막 항목으로 건너뛸 것입니다. 보안 인재 확보 및 유지를 보안 탄력성의 주요 측면으로 본 응답자는 3.8%에 그쳤습니다. 응답자들은 인재 유지를 탄력성에 영향을 미치는 사고에 중요하다고 보지 않고, 인사부의 책임이나 장기적인 목표로 보는 것 같습니다. 그러나 훈련된 보안 인력을 충분히 보유하는 것은 탄력성 있는 조직의 중요한 성공 요인입니다. 관련 내용은 나중에 설명하겠습니다.

아시겠지만 경험을 통해 보안 탄력성의 수반 사항을 인식하게 됩니다. 앞에서 응답자 중 62%가 탄력성에 영향을 미치는 보안 사고를 경험했다고 말한 것을 기억해 보십시오. 그림 6에 따르면, 해당 보안 사고로 인해 우선순위 순서가 변경되었을 수 있습니다.

그림 6: 사고 경험 유무에 따른 보안 탄력성 성과의 중요성 인식 순위



출처: 시스코 보안성과연구

손실 완화는 큰 사고를 경험하지 않은 조직에서 4위였다가 큰 사고를 경험한 조직에서 1위로 바뀝니다. 변화하는 사건에 대한 적응 및 비즈니스 성장에 보조를 맞추는 것도 마찬가지입니다. 사고 방지 및 역량 성숙도는 뒤로 밀려납니다.

인구 통계학적 특성과 기업 통계학적 특성에 따라 보안 탄력성에 대한 인식이 다른지에 대해서도 알고 싶으실 것입니다. 여기서도 긍정적인 데이터를 확인하게 됩니다. 응답자 역할을 필터로 사용하여 CISO와 보안 책임자를 기술 역할의 보안 전문가와 비교합니다.

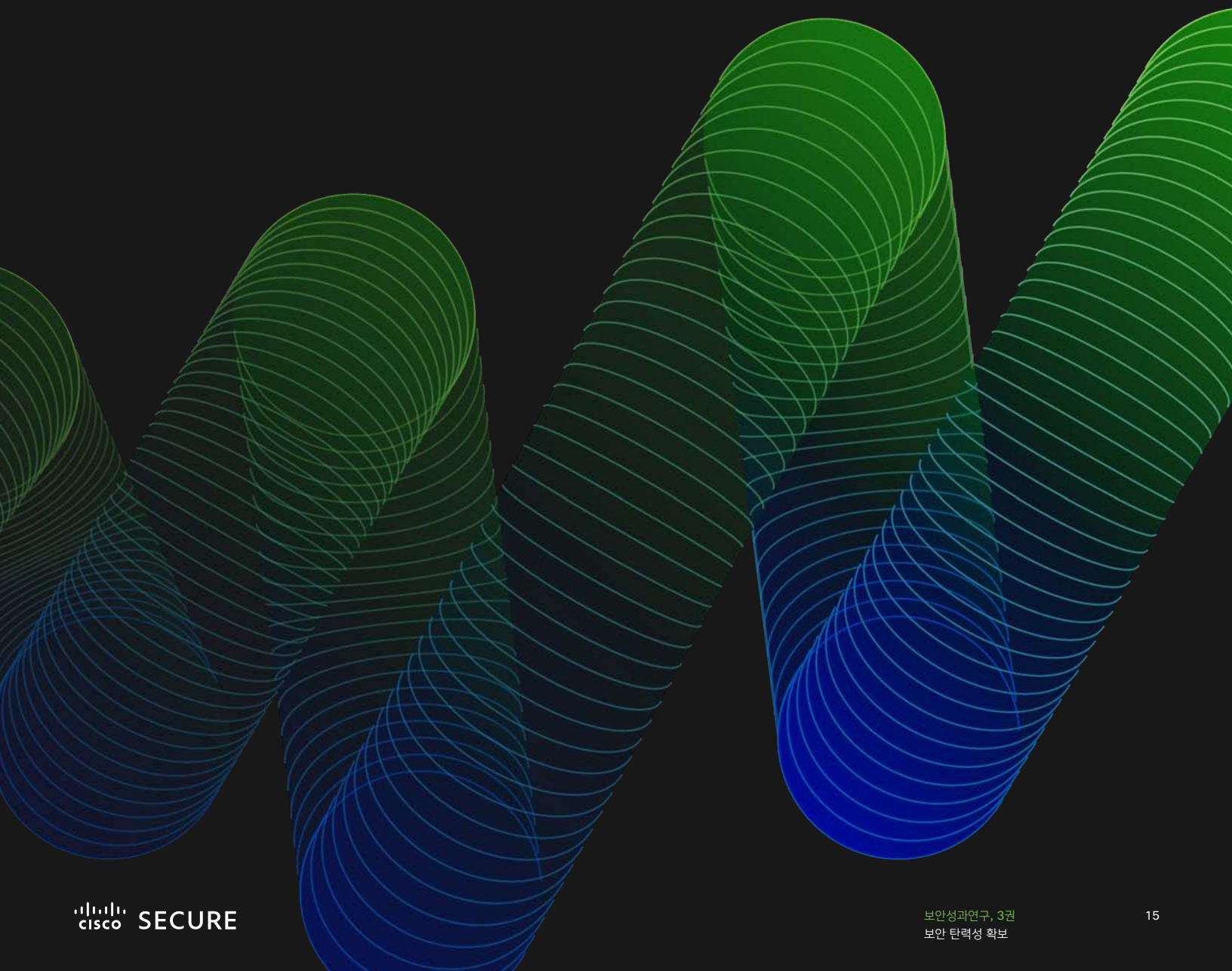
그림 7: 업무 역할에 따른 보안 탄력성 성과 중요도 인식 순위

출처: 시스코 보안성과연구

의견의 차이는 처음부터 바로 나타납니다. 보안 리더는 재정 손실을 완화하고, 사고의 확산과 범위를 억제하며, 비즈니스를 방해하지 않는 것을 우선시합니다. 각각 2위, 5위, 6위를 차지한 기술 및 운영 보안 응답자가 더 많았으며 주요 사고 예방을 가장 중요하게 여깁니다. 어느 그룹이 옳고 그르다는 것이 아닙니다. 보안 탄력성의 각기 다른 측면에 집중하는 것은 당연합니다. 하지만 모든 사람이 팀으로 협력하여 개선된 성과를 얻을 수 있게 공유된 우선순위를 설정하고 책임을 설명하는 것이 좋을 것 같습니다.

" 우리는 항시 작동하는 99.999%의 능력을 가진 시스템 구축에 대해 지겹고 철 지난 개념을 가지고 있습니다. 보안 탄력성에 대해 이야기할 때는 시스템이 작동을 중단할 경우 기술적인 문제가 있어도 계속 작동하는 시스템을 구축하는 데 실패하는 경향이 있습니다."

— Dave Lewis,
Cisco Secure 자문 담당 CISO



보안 탄력성의 상태

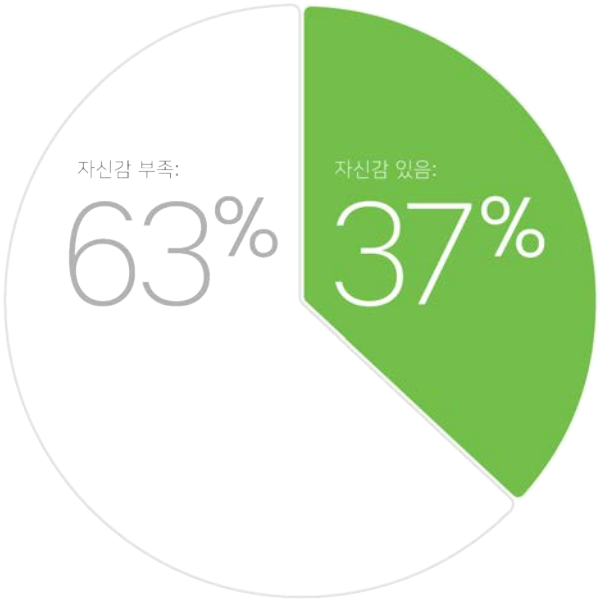
최악의 (그러나 발생 가능성이 있는) 사이버 사고가 오늘 발생한다면 조직이 얼마만큼의 탄력성을 유지할 것이라고 확신하는지 응답자들에게 물었습니다.

1/3이 조금 넘는 이들은 강한 자신감을 나타냈고, 나머지 2/3는 조직 운영 상태에 대해 어느 정도 의구심을 나타냈습니다.

이러한 주관적인 질문을 통해 보안 탄력성의 상태에 대한 직감을 확인할 수 있지만, 목표를 달성하려면 좀 더 구체적인 방식으로 측정해야 합니다. 응답자가 원하는 일련의 보안 탄력성 성과에 대한 의견을 확보했으므로, 이러한 성과를 달성하기 위한 조직의 상태를 살펴보겠습니다.

응답자들에게 4점 만점 기준으로 각 목표에 대한 조직의 성과를 평가하기를 요청했습니다(실패 | 고투 | 수행 | 탁월). 이 항목을 보다 객관적으로 평가할 수 있도록 각 성과에 대한 설명과 함께 실패 및/또는 탁월에 대한 예시를 제공했습니다. 이러한 설명과 예시는 해당 사항을 보다 자세히 알고자 하거나 조직 내에서 사용할 수 있게 조정하려는 사용자를 위해 부록 B에 포함되어 있습니다.

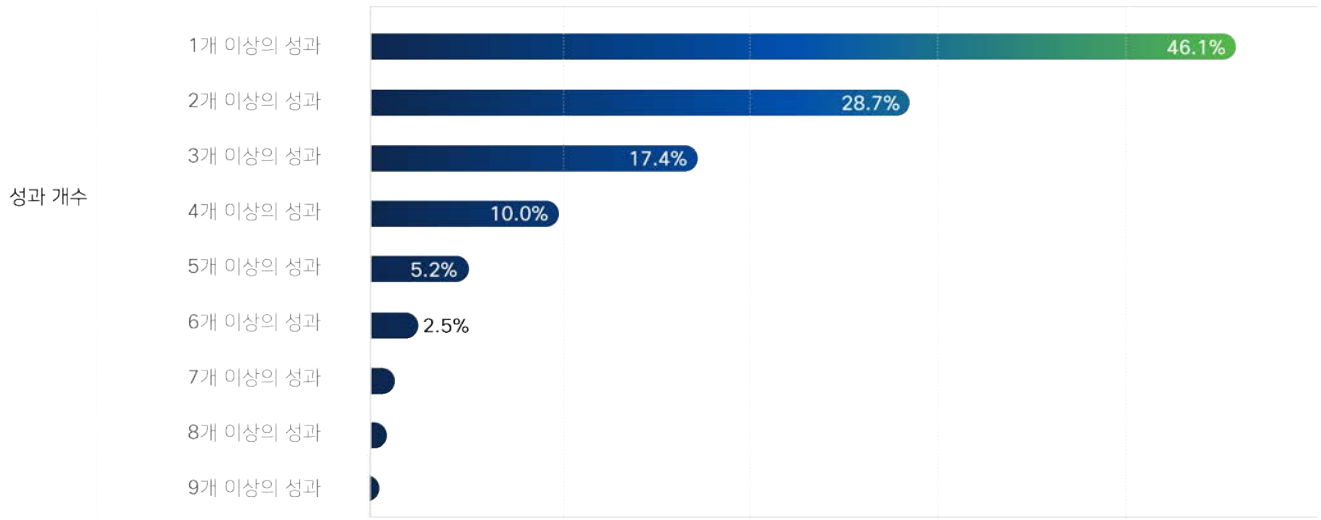
그림 8: 최악의 사이버 사고 중에도 탄력성을 유지할 수 있는 능력에 대한 신뢰



출처: 시스코 보안성과연구

일반적으로 응답자 대부분은 자신의 조직이 적어도 전체적으로 " 수행" 중이라고 답했습니다. 그러나 그렇다고 해서 보안 탄력성의 세계에서 모든 것이 괜찮다고 받아들이지는 마십시오. 그림 9에서 볼 수 있듯이, 설문조사 참가자 중 약 절반은 조직이 9가지 보안 탄력성 성과 중 하나 이상을 달성하는 데 고군분투하거나 완전히 실패했다고 답합니다. 1/4 이상이 최소 2개의 성과 달성과 관련하여 어려움을 겪고 있으며, 10%는 최소 4가지 성과로 인해 어려움을 겪는다고 합니다. 이를 통해 보안 탄력성의 핵심 영역에서 성취도가 낮은 조직이 많다는 결론을 내렸습니다.

그림 9: 보안 탄력성 성과를 내느라 어려움을 겪는 조직의 비율



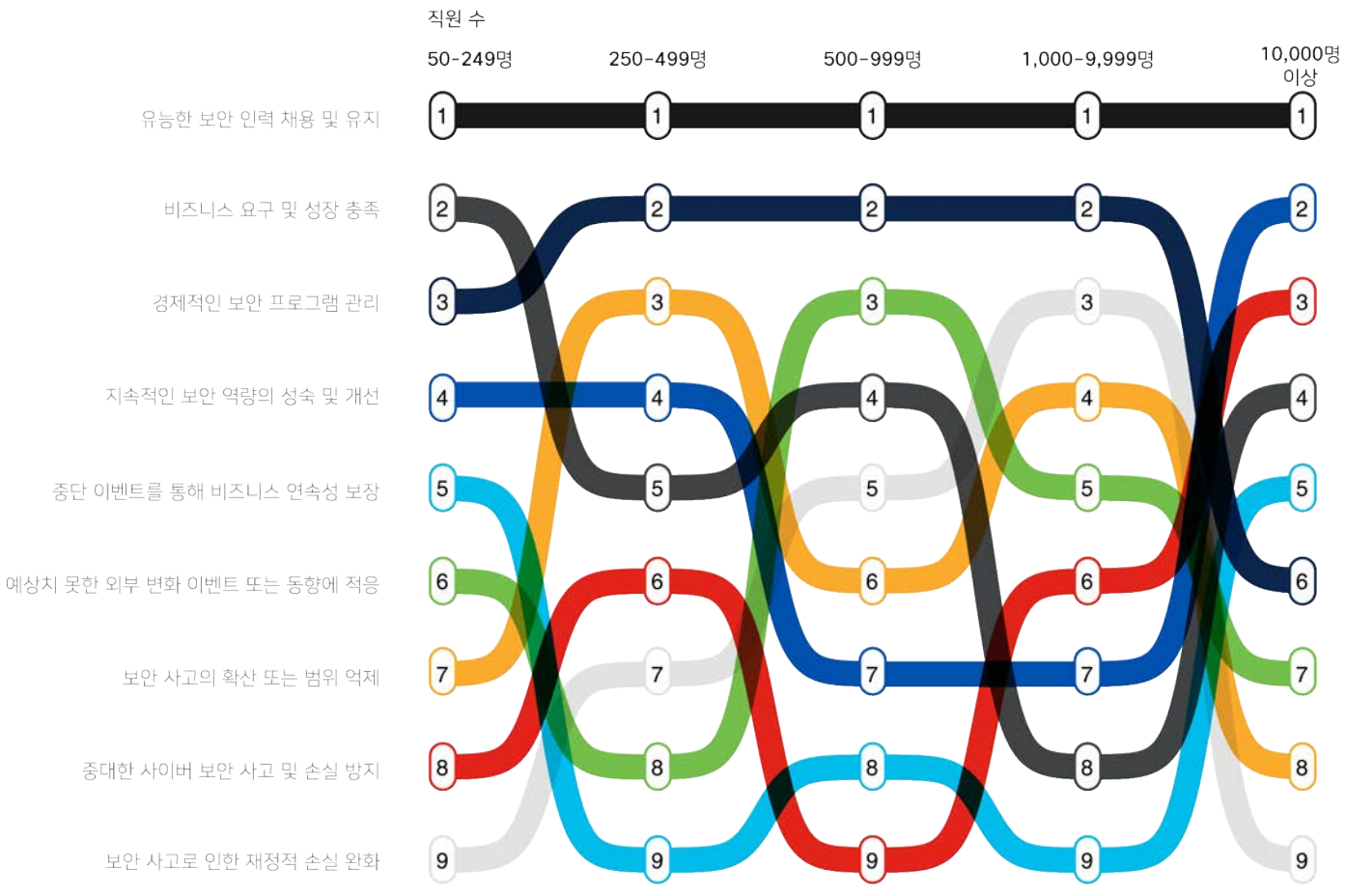
출처: 시스코 보안성과연구

앞에서 살펴본 바와 같이 이러한 보안 탄력성 성과의 상대적 중요성에 대한 인식이 다르기 때문에 조직 유형마다 성과도 다르다는 사실은 전혀 놀랍지 않습니다. 예로, 그림 10에서는 각기 다른 조직 규모에서 성과를 내느라 어려움을 겪고 있는 참가자의 비율을 비교하고 있습니다. 크고 작은 기업들은 보안 인력을 채용하고 유지하는 것이 가장 큰 과제라는 데 동의하지만, 합의는 여기에서 그칩니다.

이러한 견해가 특히 흥미로운 것은 조직이 성장함에 따라 어려움을 겪는 영역이 변하는 것 같기 때문입니다. 예를 들어, 재정 손실을 줄이는 것은 규모가 가장 작은 기업들에게 가장 덜 어려운 일로 알려져 있습니다. (자금을 잃는 것보다 폐업이 더 걱정되기 때문일지도 모르겠습니다.) 그러나 직원 수가 1,000~9,999명인 조직에서 이 항목은 상위 3위 안에 진입합니다. 그러다가 대기업에서는 최하위로 추락합니다. (수익이 높으므로 추가적인 재정적 보안이 갖춰져 있기 때문일 수도 있겠습니다.)

반면에, 어떤 항목은 성장에 관계없이 절대 변하지 않는 것 같습니다. 위에서 언급한 것처럼, 크고 작은 조직은 다른 어떤 성과보다 보안 인재 영입 및 유지에 어려움을 겪습니다. 이 부분은 만장일치로 해당 성과를 보안 탄력성에 대한 가장 낮은 우선순위로 평가하기 때문에 다소 모순적입니다. 어쩌면 자기실현적 예언인지도 모르겠습니다. 아니면 그저 직설적인 실용주의일 수도 있습니다. *("물론, 좋은 인력을 유지하는 것은 어렵지만, 큰 사고나 손실을 피하는 것에 더 신경쓰고 있습니다.")*

그림 10: 조직 규모별 가장 어려운 보안 탄력성 성과 순위



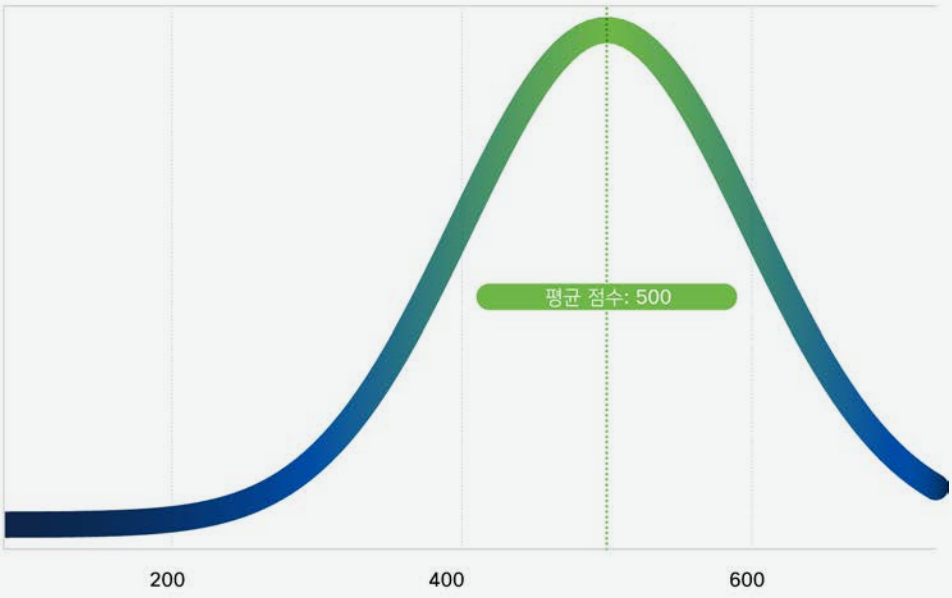
출처: 시스코 보안성과연구

개별 성과에 대한 평가와 더불어 각 참여 조직의 보안 탄력성에 대한 전반적인 수준을 측정하고자 했습니다. 그래서 9가지 성과 전반에서 각 조직의 성과를 바탕으로 보안 탄력성 점수를 만들었습니다. 그 방법에 관해서는 아래 상자를 확인하십시오. 그러나 핵심은 점수가 높을수록 더 많은 수의 보안 탄력성 성과에서 더 뛰어난 성과를 보인다는 것입니다. 이 점수를 다음 섹션에서 광범위하게 사용하여 보안 탄력성 향상에 대한 다양한 성공 요인의 효과를 측정할 것입니다.

전반적인 보안 탄력성 점수 측정

각 성과를 평가하는 것 외에도, 전체 보안 탄력성을 측정하는 척도로서 9개의 성과 모두에 대한 조직의 성취 수준을 파악하는 총 점수를 집계하고자 했습니다. 이를 '보안 탄력성 점수'라고 하며, 본 보고서에서 여러 번 참조되어 있는 것을 확인하실 수 있습니다.

그림 11: 참가자 전반의 보안 탄력성 점수 분포



출처: 시스코 보안성과연구

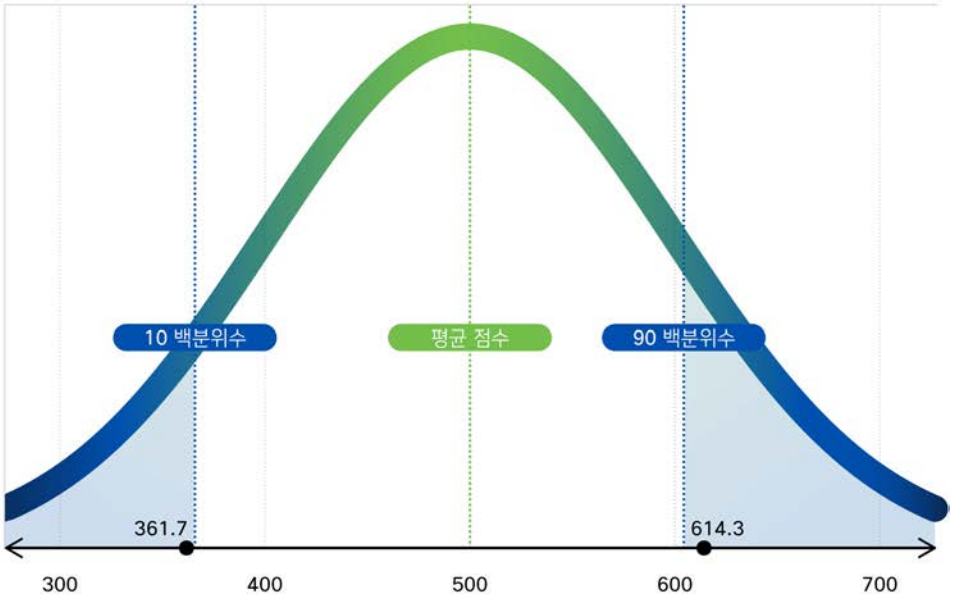
점수를 산정하기 위해 문항반응이론(Item Response Theory)이라는 통계학 기법을 사용했습니다. (마지막 권의 보안 성과 점수에서도 동일했습니다.) 이 기법을 통해 모든 성과 항목에 걸친 실적에 따라 조직에 점수를 매기면서 성과 항목마다 달성의 난이도가 다르다는 사실을 반영할 수 있습니다. 검증된 이 기법을 통해 표준화된 테스트 점수를 산정할 수 있습니다. 점수의 절대적인 수치에 구체적인 의미는 없지만, 다양한 프로그램을 비교할 수 있는 신뢰할만한 근거입니다. 보안 탄력성 점수 분포는 그림 11과 같으며, 평균은 500에서 떨어졌습니다.

탄력성을 위한 7가지 성공 요인

이제 여러분이 기다리시던 부분이거나 읽으시던 부분입니다. 4,700개 이상의 각 조직에 대한 9개의 성과에서 전체 보안 탄력성을 나타내는 점수를 통해 이를 개선하는 방법을 살펴보겠습니다. 우리는 잠재적인 조직 요소, IT 요소, 보안 요소를 분석하여, 이러한 요소가 더 강력한 보안 탄력성과 어떤 상관관계를 갖는지 테스트했습니다.

이 프로세스를 통해 보안 탄력성을 위한, 데이터에 기반한 성공 요인 7가지를 파악했습니다. 이를 통해 얼마만큼의 차이가 발생했을까요? 질문해 주셔서 감사합니다. 이러한 요소를 나타내는 조직은 보고서의 모든 참가자에 대해 측정한 모든 보안 탄력성 점수 중 상위 10% 이내의 점수를 받았습니다. 반면, 해당 사항 중 대다수가 빠진 조직은 하위 10 백분위수로 떨어집니다. 어떤 조직도 그 수치를 원하지 않습니다.

그림 12: 7가지 성공 요인을 준수할 때 전체 보안 탄력성 점수에 미치는 영향



출처: 시스코 보안성과연구

이러한 성공 요인을 구현하는 조직은 탄력성이 10 백분위수에서 90 백분위수로 크게 개선됩니다.

그렇다면 보안 탄력성 강화를 위한 행운의 7가지 요소는 무엇이며, 어떻게 하면 이러한 이점을 누릴 수 있을까요? 미리 말씀해 두자면 행운과는 관계가 없습니다! 덴젤 워싱턴은, " 행운이란 준비된 자가 기회를 만났을 때 차지하는 것이다" 라고 했습니다. 이 섹션의 나머지 부분은 이러한 준비를 하시도록 도와드릴 것입니다.

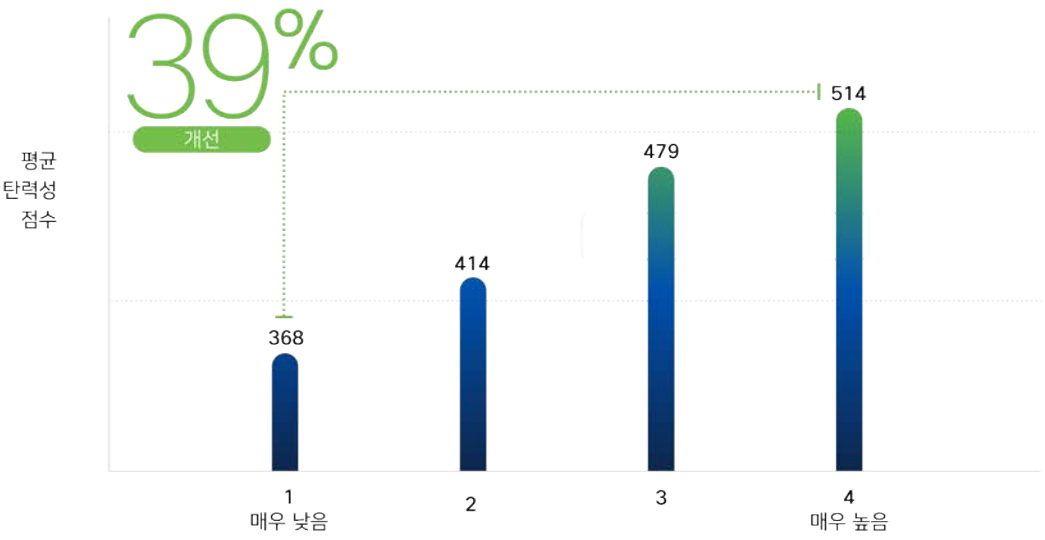
1. 임원진 지원 구축

이 요소가 사이버 보안 세계에서 다소 진부하다는 점은 인정하지만, 바로 무시할 수 없는 효과가 있습니다. 최고위 임원진의 지원이 부실하다고 답하는 조직은 강력한 지원을 받는 조직보다 보안 탄력성 점수가 39% 낮습니다. 물론 진짜 문제는 임원진의 지지를 얻는 방법입니다.

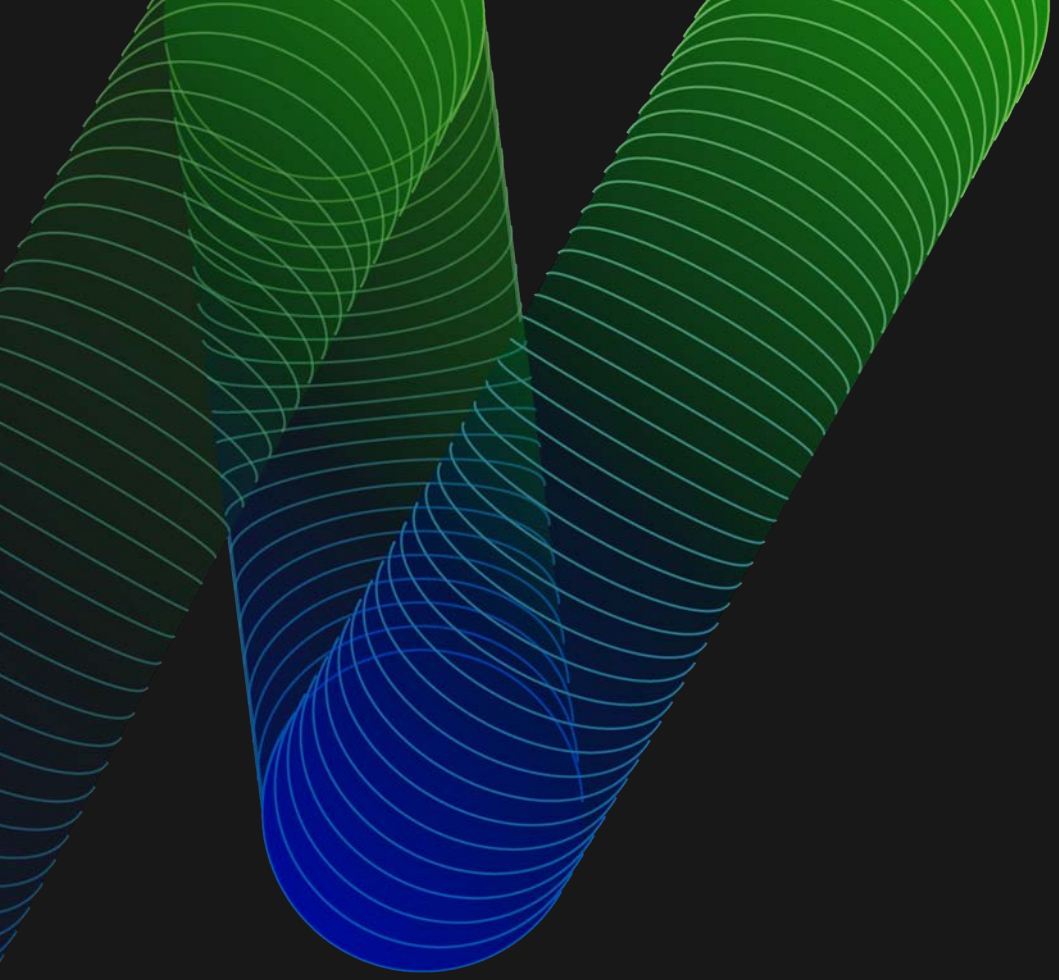
데이터에 따르면 비즈니스 핵심 사명과 긴밀하게 연계된 보안 프로그램은 임원진 수준의 지원이 비교적 탄탄할 뿐 아니라 탄력성도 우수합니다(전체 점수 대비 +32%). 따라서 최고위 임원진과의 연결은 비즈니스 작동 방식과 보안 이니셔티브 작동 방식을 개선하는 방법에 대한 명확한 이해를 기반으로 합니다. 결국, 지원은 어떤 관계에서든 양방향으로 이루어집니다.

이 문서에서는 관계라는 주제에 대해 설명하면서 또 다른 분석 사항을 말씀드리겠습니다. 우리는 응답자들에게 조직 중 어느 위치에서 보안 탄력성에 대한 책임을 지는지 물었습니다. 그리고 대부분의 경우, 보고 라인은 큰 차이가 없는 것 같습니다. 그러나 CEO, CRO(Chief Risk Officer, 최고리스크관리책임자), CISO가 긴밀하게 관여한 조직은 다른 C-레벨 임원진(예: CIO, COO, CTO, CFO)이 책임을 맡은 조직보다 보안 탄력성 점수가 훨씬 높다는 사실을 알게 되었습니다.

그림 13: 임원진 지원이 보안 탄력성에 미치는 영향



출처: 시스코 보안성과연구



" CISO는 반드시 임원진과의 관계를 강화해야 합니다. 비즈니스 조정을 개선하고 예산 및 인원수에 대한 임원진의 승인을 확보하는 조직은 보안 탄력성을 향상할 수 있습니다. 좋은 관계는 좋은 보안 프로그램으로 이어지고, 좋은 프로그램은 좋은 관계로 이어집니다."

– Wolfgang Goerlich,
시스코 자문 CISO

2. 보안 문화 조성

보안 탄력성을 개선하고자 하는 리더는 임원진 지원을 확보하면서 시작할 수 있지만, 거기서 그쳐서는 안 됩니다. 조직 전체에 보안 문화를 조성하기 위해 노력해야 합니다. 데이터에 따르면 그렇게 할 수 있는 조직이 보안 문화가 빈약한 조직에 비해 탄력성 점수가 46% 상승하기 때문입니다.

±46% 보안 문화가 빈약한 조직과 우수한 조직 사이의 평균 탄력성 점수 차이

물론 이는 말처럼 쉬운 일이 아닙니다. 그리고 강력한 보안 문화가 무엇을 의미하는지, 그리고 보안 문화를 이 보고서에서 어떻게 평가했는지에 대한 질문은 타당합니다. 우리는 응답자가 조직 보안 문화의 강점을 평가하고 순위를 매기는 데 도움이 되도록 다음과 같은 지침을 제공했습니다.

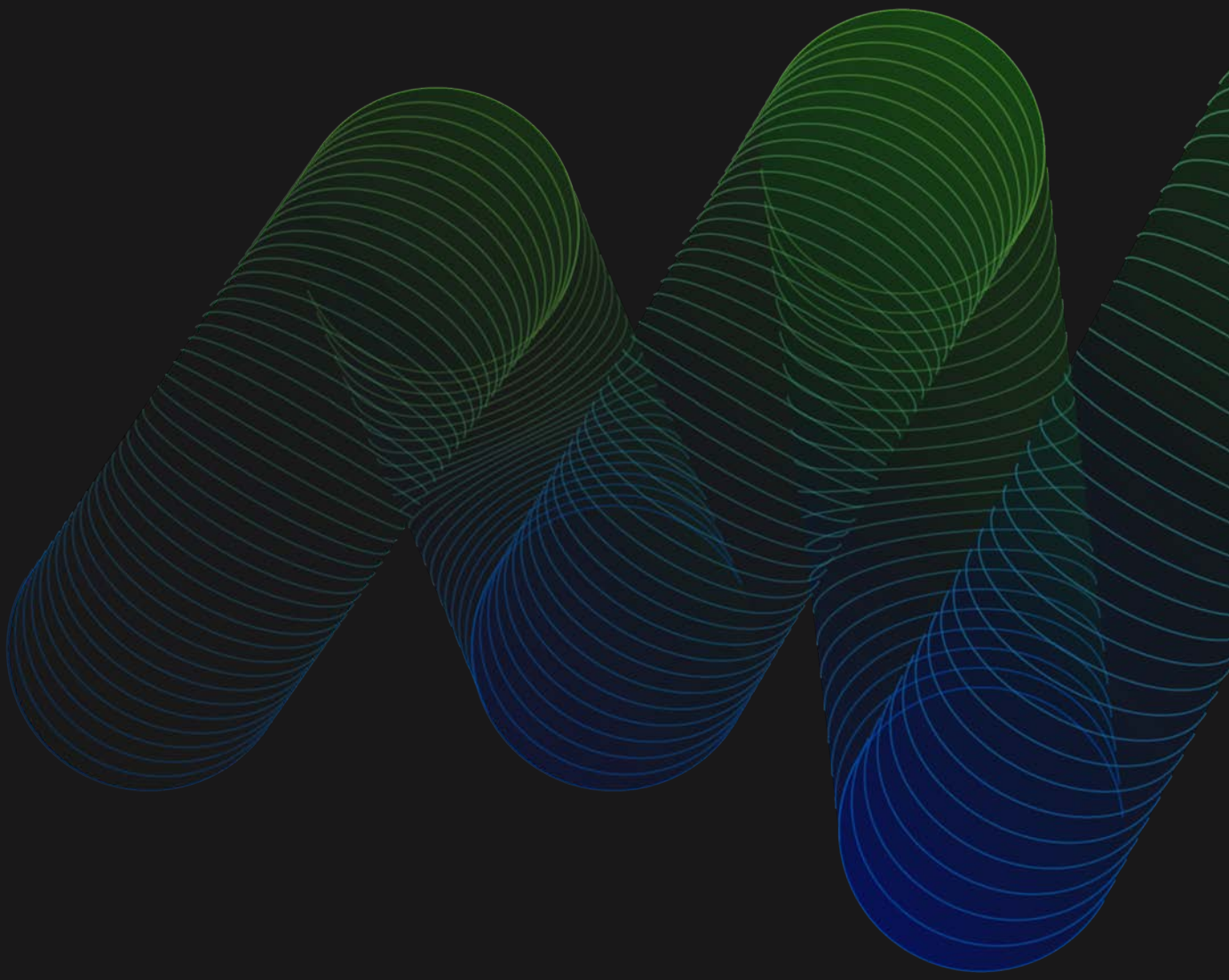
> 강력한 보안 문화에서는 직원을 문제가 아닌 해결책의 일부로 여깁니다. 보안 담당 직원은 조직의 맥락에서 자신의 역할을 이해하고 비보안 담당 직원 역시 자신이 할 역할이 있음을 알고 있습니다. 이는 피싱 시도, 잠재적 악성코드 및 기타 사고를 정기적으로 보고함으로써 확인 가능합니다. 직원 만족도 설문이나 퇴사 인터뷰에서 보안은 부정적인 주제가 아닙니다. 반대로 빈번한 보안정책 위반과 회피책은 보안 문화가 빈약하다는 증거입니다.

그것은 각 조직마다 강력한 보안 문화에 대한 관점이 다를 것이므로 이를 자세히 설명하기 위한 것은 아닙니다. 그러나 적어도 응답자들이 보안 문화의 강점을 평가할 때 염두에 두었던 점을 파악함으로써, 각자 측정할 수 있기를 바랍니다.

설명의 행간을 읽다 보면 보안 프로그램이 정책과 근거를 조직의 나머지 직원들에게 명확하게 전달하는 것이 중요하다는 점을 알 수 있습니다. 이러한 측면에서 조직에 높은 점수를 준 응답자는 보안 프로그램이 하고 있는 일과 그것을 하는 이유를 설명할 수 없다고 응답한 응답자보다 보안 탄력성 점수가 27% 높은 것으로 나타났습니다. 각자가 사용하는 청사진이 다를 때 강력한 문화를 구축하기란 어렵습니다.

" 보안 의식이란 주제는 보안 문화에 대한 강조로 대체되어 사라지고 있으며, 조직의 DNA를 바꾸고 모든 동료가 보안 대가족의 일원이 되고 있습니다. 단순 교육은 필수적인 컴플라이언스에 대한 실천인 동시에 조직의 가치를 소통하고 변화시키는 것은 이제 많은 CISO가 중요한 목표로 간주합니다."

— Richard Archdeacon,
시스코 자문 담당 CISO



3. 예비 자원 유지

앞서 살펴본 바와 같이 우수한 보안 인력을 채용하고 유지하는 것이 가장 덜 중요한 보안 탄력성 성과이자 가장 어려운 성과로 인식되는 경향이 많았습니다. 보안성과연구 1권 및 2권에서는 사이버 보안 프로그램의 인력 요소와 관련된 측정 가능한 이익을 언급했으며, 3권 역시 다르지 않습니다.

놀랍게도 조직 내 총 직원 수를 통제하더라도 전체 보안 직원의 규모와 보안 탄력성 수준 간에 강력한 상관관계가 발견되지 않았습니다. 그러나 다른 점은 예상치 못한 사이버 사고에 더 철저히 대응하기 위해 내부 인력과 자원을 초과 유지하는 것입니다. 이것이 가능한 조직은 필요할 때 활용할 수 있는 " 유연한" 자원이 없는 조직보다 보안 탄력성 점수가 평균 15% 더 높습니다.

이미 기본 보안 인력을 고용하고 유지하는 것이 어려운 상황에서 조직은 어떻게 해야 내부 자원을 초과 유지할 수 있을까요? 안타깝게도 이번 설문조사에서는 관련 내용을 자세하게 알아보지 않았지만, 해당 사항은 현재 향후 연구 대상으로 예정되어 있습니다.

±15% **사고 대응을 위해 내부 인력을 초과 유지하는 조직과 그렇지 않은** 조직 간의 평균 탄력성 점수 차이

±11% **외부 사고 대응 서비스를 유지하는 조직과 그렇지 않은** 조직 간의 평균 탄력성 점수 차이

조직에서 예상치 못한 사고를 처리하기 위해 내부 직원을 초과 유지하기 어려운 상황이라도 희망을 버리지는 마십시오. 이번 분석에서는 외부 사고 대응(IR) 서비스를 유지하는 기업의 보안 탄력성이 평균 11% 높다는 사실도 지적합니다. 전화 한 통이면 도움을 받을 수 있도록 신뢰할 수 있는 IR 서비스 제공업체와 유지 계약을 체결하는 것을 고려해 보십시오.

내부 자원이나 외부 IR 서비스가 추가 이점을 제공한다면, 두 가지를 함께 활용하는 것이 훨씬 더 좋다고 생각하실지도 모릅니다. 이는 사실인 것 같습니다. 주요 사이버 사고에서 내부 및 외부 자원이 모두 준비되어 있으면 둘 중 하나만 보유한 것보다 보안 탄력성 점수가 13% 더 높아집니다.

4. 하이브리드 클라우드 환경 간소화

클라우드 아키텍처와 마이그레이션은 IT 팀뿐만 아니라 보안 팀에서 상당 기간 중요한 주제였습니다. 많은 기업이 인프라에서 소프트웨어까지 클라우드에 올인한 반면, 일부 기업은 온프레미스에서 요지부동입니다. 그러나 이러한 전략 중 어느 것이 보안 탄력성에 더 도움이 될까요? 정답은 둘 다라고 생각하십니까?

참가자들에게 일반적으로 IT 인프라를 온프레미스에서 호스팅하는지, 클라우드에서 호스팅하는지 (또는 다양한 수준의 하이브리드 모델에서 호스팅하는지) 물어봤습니다. 그런 다음 답변과 각 조직의 보안 탄력성 점수를 서로 연관시켜 보았습니다. 클라우드를 많이 사용하는 조직은 평균 526점, 주로 온프레미스를 사용하는 조직은 평균 525점이었습니다. 즉, 온프레미스를 많이 사용하는 환경과 클라우드를 많이 사용하는 환경 간에는 보안 탄력성 성과에 차이가 없었습니다.

±15% 관리하기 쉬운 하이브리드 클라우드 환경과 관리하기 어려운 하이브리드 클라우드 환경 전반에서 평균 탄력성 차이

차이가 발견될 때는 온프레미스 환경과 클라우드 환경 *각각을 비교할 때*입니다. 초기 하이브리드 모델의 조직은 주로 온프레미스를 사용하는 조직보다 보안 탄력성 점수가 평균 14% 낮습니다. 영화 '사랑의 블랙홀'에서 네드 라이어슨은 " (클라우드로 향하는) 첫 걸음을 조심하세요. 아주 고약하거든요!" 라고 말합니다.

그러나 클라우드로의 첫 걸음을 조금 덜 힘들게 할 수 있다는 증거가 있습니다. 별도의 질문에서 하이브리드 환경의 관리·보안이 더 쉽다고 평가한 조직은 클라우드 마이그레이션의 초기 단계를 나타내는 탄력성에 대한 부정적인 타격을 완화하는 것 같습니다. 해당 기업들의 탄력성 점수는 14%가 아니라 8.5% 감소하는 데 그쳤습니다. 또한 클라우드 채택 수준이 높아짐에 따라 하이브리드 환경의 관리 간소화라는 이점도 강화됩니다.

보다 광범위한 하이브리드 환경을 보유한 조직은 관리를 간소화할 수 있는 경우 탄력성 점수가 통계적으로 온프레미스(또는 전체 클라우드) 기준과 동등한 수준입니다. 그렇지 않은 조직은 관리하기 어려운 하이브리드 상태에 빠지고 이러한 탄력성 이점은 사라집니다. 전반적으로, 관리하기 어려운 초기 하이브리드 클라우드 환경과 관리하기 간편한 고급 클라우드 구축 간 탄력성 점수는 15% 차이를 보입니다.

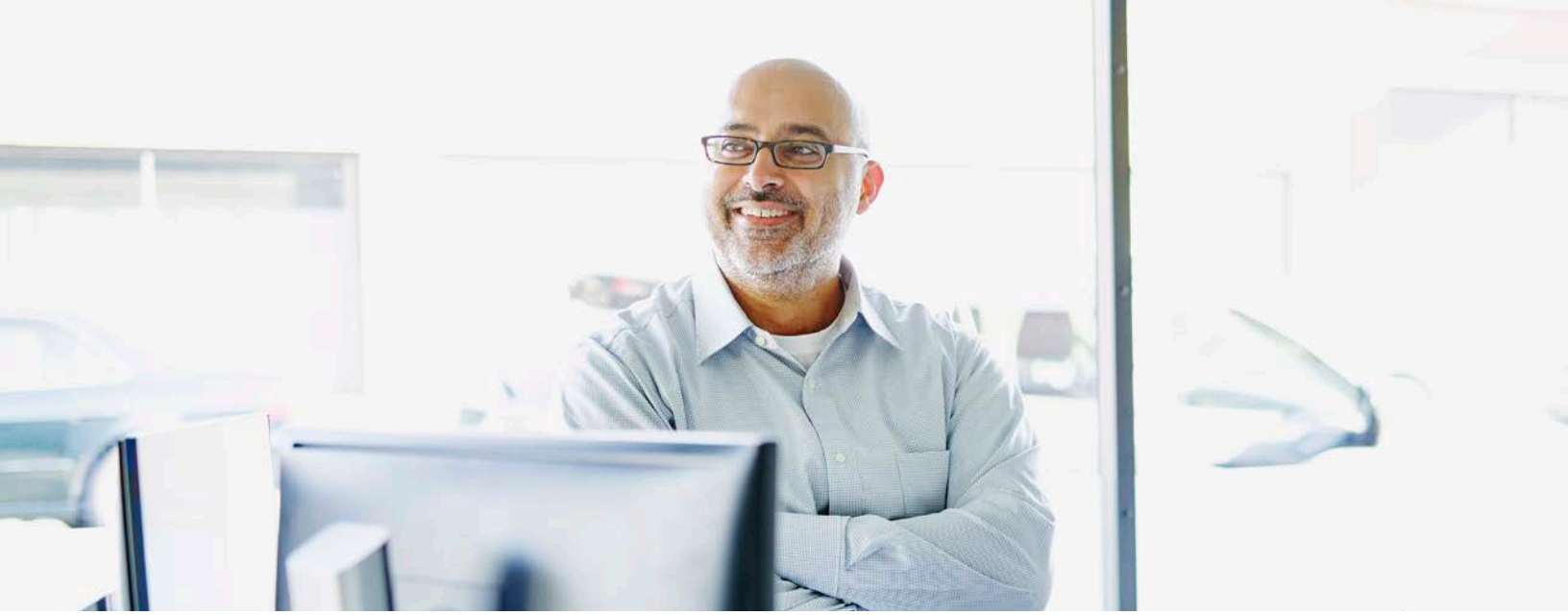
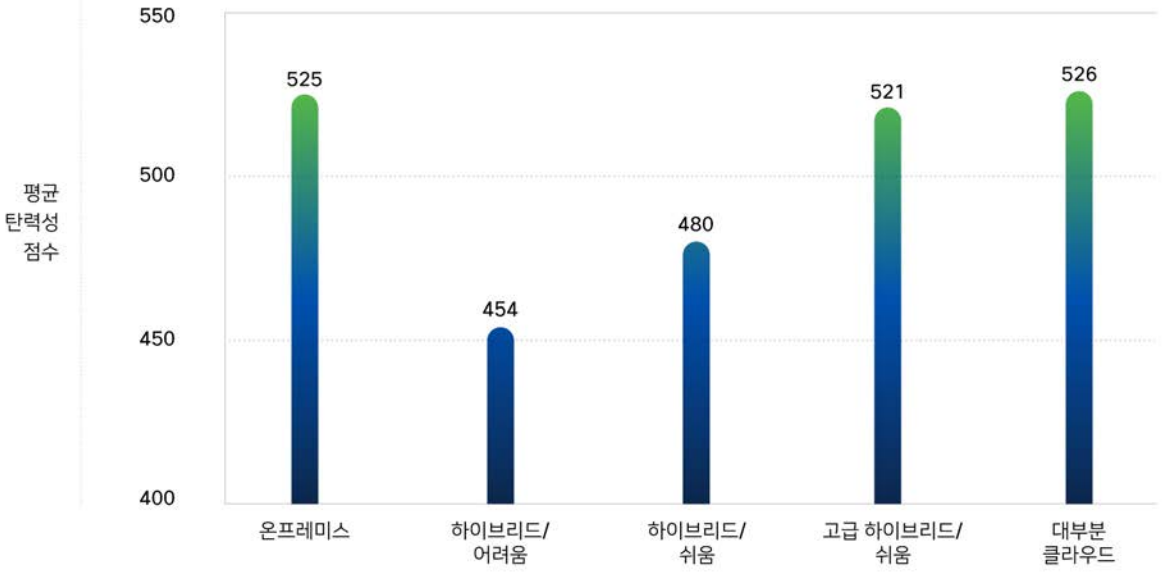


그림 14: 클라우드 채택 및 관리 용이성이 보안 탄력성에 미치는 영향

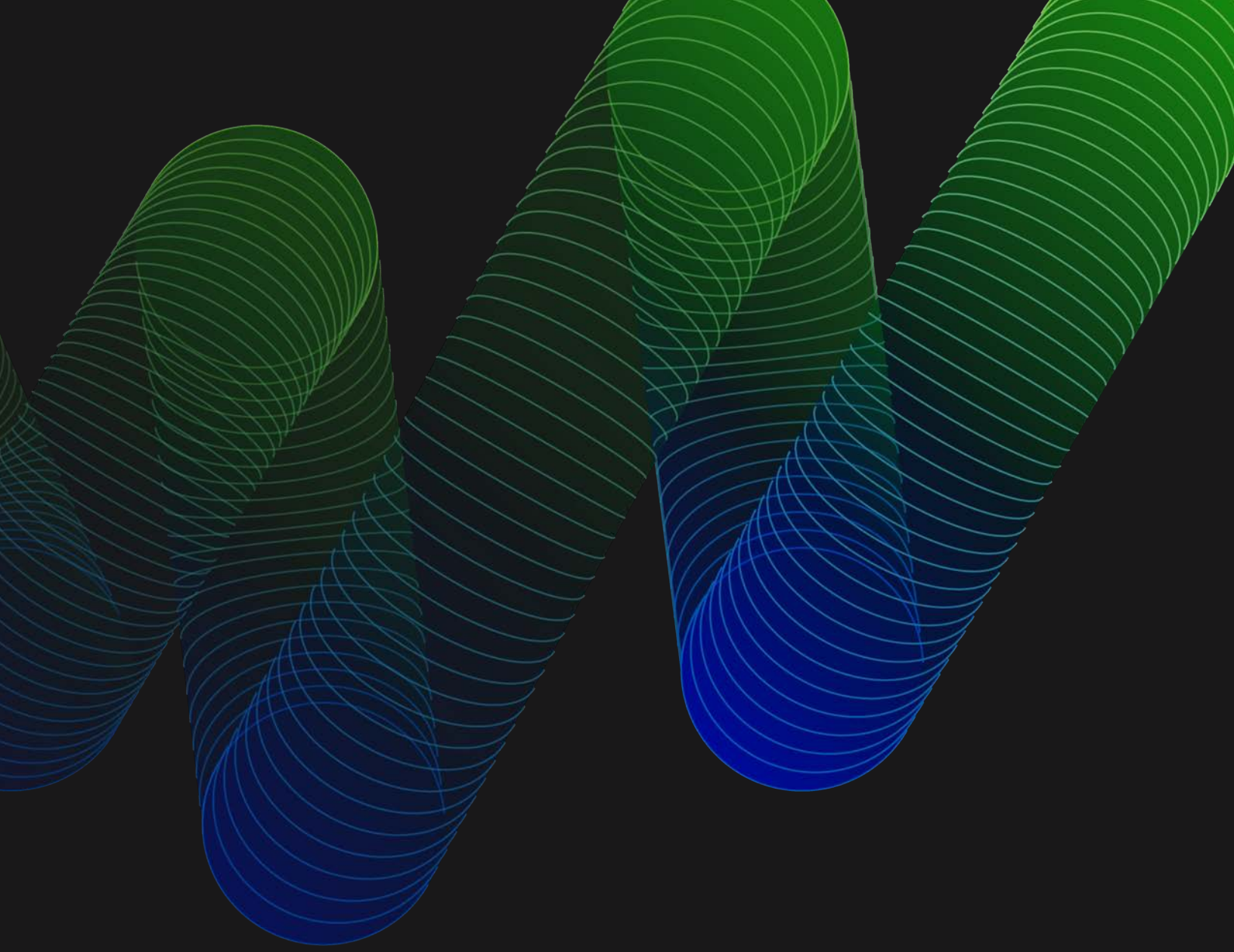


인프라 마이그레이션 마일스톤

출처: 시스코 보안성과연구

이를 통해 단순하고 마찰이 없는 상태를 유지하는 것이 클라우드로 전환하기 위한 핵심 성공 요인이라고 추론할 수 있습니다. 하이브리드 클라우드 구축은 클라우드 전환 시 꼭 필요하기 때문에, 이렇게 복잡한 환경을 관리하는 데 적합한 도구와 서비스를 확보하면 전환하는 내내 조직을 안전하고 탄력적으로 유지할 수 있습니다.

조직의 규모에 관계없이 여기서 설명하는 일반적인 패턴이 적용된다는 점은 눈여겨볼만 합니다. 모든 규모의 조직에서 클라우드와 온프레미스 극한 환경 간의 보안 탄력성에는 큰 차이가 없습니다. 그러나 중견·중소기업뿐 아니라 대기업도 하이브리드 클라우드 인프라에서 탄력성에 관련된 어려움을 겪고 있습니다. 한 가지 다른 점은 대기업이 해당 환경을 복잡하고 관리하기 어렵다고 평가할 가능성이 3배 높다는 것입니다. 즉, 클라우드로의 전환을 제대로 관리하지 않으면 보안 탄력성에 더 큰 타격을 줄 수 있습니다.



"대부분 보안 담당자들이 온프레미스에서 클라우드로 신속하게 전환하는 데에는 영향을 미치지 못한다는 것이 문제입니다. 기술을 바꿀 수 없다면, 유일하게 활용 가능한 수단은 사람과 프로세스입니다."

— Helen Patton,
Cisco Security Business Group의 CISO

5. Zero Trust 채택 극대화

오늘날의 비즈니스 환경에서는 어디에서나 근무 가능하므로 비즈니스를 완벽하게 보호하려면 보안이 어디에나 존재해야 합니다. 기업 네트워크 내부의 모든 것(디바이스, 사용자, 인프라 등)을 신뢰하는 기존 보안 접근 방식으로는 그런 수준의 보호 기능을 제공할 수 없습니다. 따라서 맹목적 신뢰를 없애는 접근법이 생겨났습니다. Zero Trust 모델은 모든 애플리케이션을 보호하는 사용자 지정 보안 정책과 함께 각 액세스 시도에 대한 인증 및 지속적인 모니터링을 통해 사용자와 디바이스에 신뢰를 구축합니다.

그렇다면 문제는 Zero Trust 모델이 보안 탄력성을 개선한다는 증거가 있느냐는 것입니다. 그리고 그 질문에 대해 기쁘게 " 그렇습니다" 고 대답할 수 있습니다. 성숙한 Zero Trust를 구현했다는 응답자들은 이러한 여정을 시작하지 않은 조직보다 보안 탄력성을 30% 높였습니다. 또한 Zero Trust는 앞에서 논의한 9가지 보안 탄력성 성과 중 8가지가 훨씬 더 큰 성공 비율을 보여주는 것과 관계가 있었습니다.

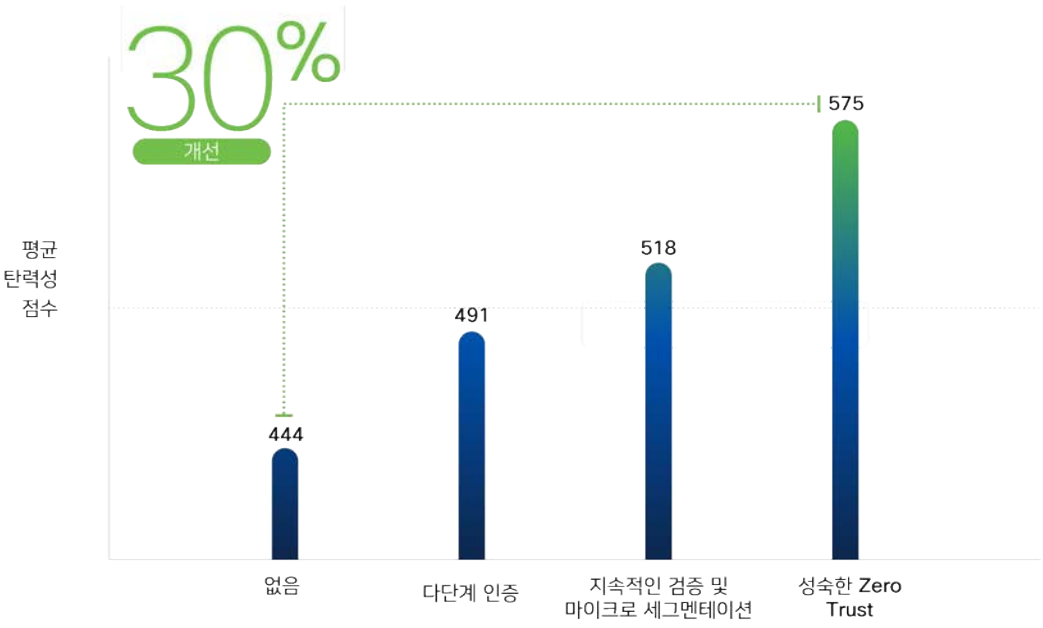
±30% 성숙한 Zero Trust를 구현하지 않은 조직과 구현한 조직 간의 평균 탄력성 점수 차이

성숙한 Zero Trust 구현은 하룻밤 사이에 이루어지지 않으며, 탄력성에 대한 이점을 한꺼번에 전부 얻을 수도 없습니다. 단계별로 구축됩니다. 이 보고서에 구현 여정의 지도를 상세하게 작성할 공간은 없지만, 그 여정에 착수하는 데 관심이 있는 이들을 지원할 자원은 많습니다. 우리가 할 일은 성숙한 Zero Trust 채택의 점진적 이점을 입증하기 위한 핵심 단계를 강조하는 것입니다.

많은 조직에서 Zero Trust 여정의 첫 번째 단계는 다단계 인증(MFA)을 통해 사용자와 디바이스를 확인하는 것입니다. 이번 응답자 중에서 MFA를 롤아웃하는 경우는 보안 탄력성 점수가 11% 향상되었습니다.

Zero Trust 여정을 계속하는 많은 조직은 워크로드의 마이크로 세분화와 함께 사용자와 디바이스에 대한 지속적인 검증을 구현할 것입니다. 데이터에 따르면, 이 경우 보안 탄력성 점수가 6% 추가되는 것으로 나타났습니다. 이런 이점을 무시하지 말고, 기본 점수가 높을수록 큰 비율의 상승이 더 어려워진다는 것을 기억하십시오.

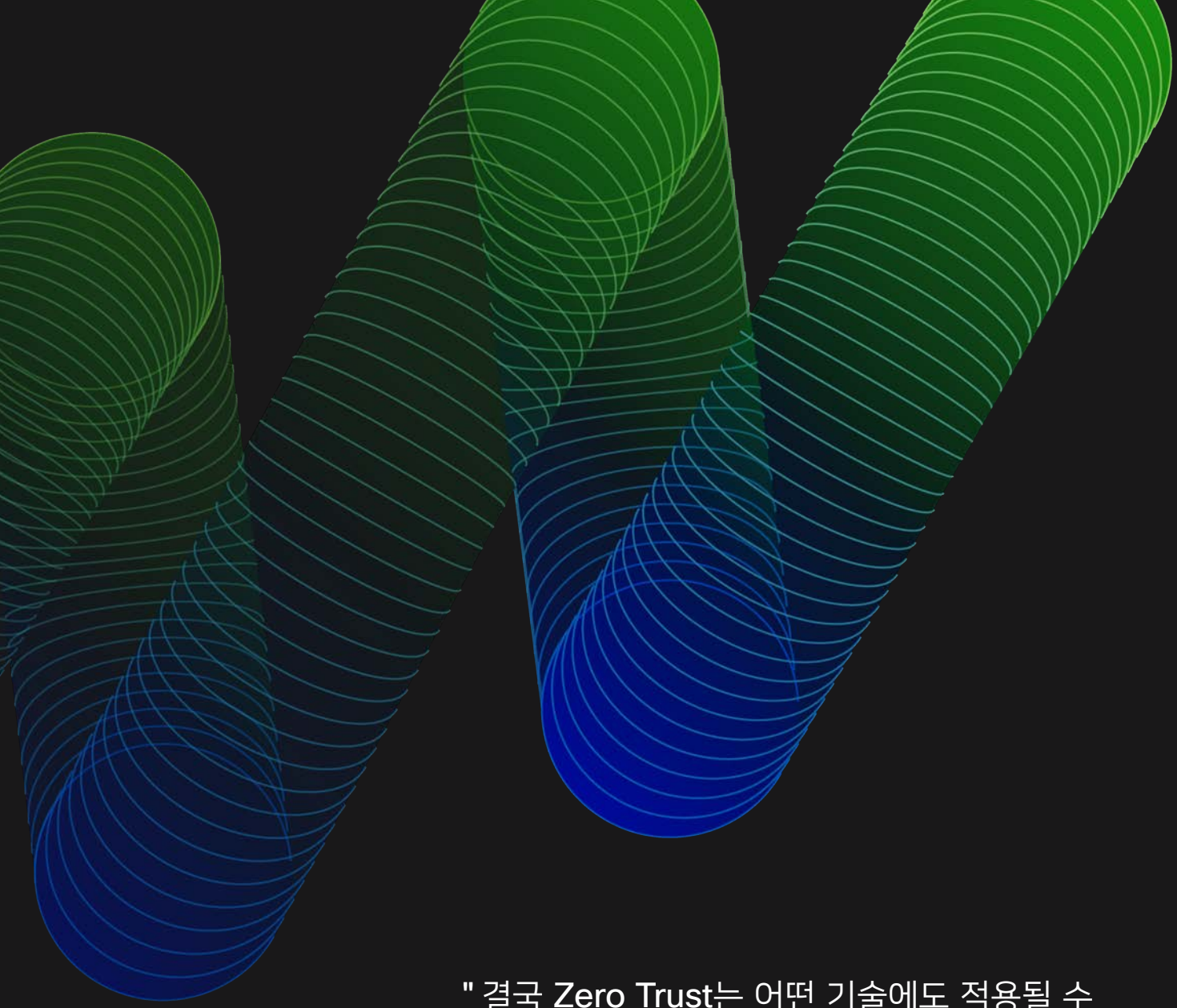
그림 15: Zero Trust 구현 마일스톤이 보안 탄력성에 미치는 영향



Zero Trust 구현 마일스톤

출처: 시스코 보안성과연구

Zero Trust 여정의 마일스톤을 하나 더 살펴봅시다. 이 마일스톤은 결승점에 가까워지고 있습니다. 여기서 조직은 적응형 정책, 광범위한 모니터링, 사용자 워크플로우 조정을 통해 MFA, 지속적인 검증 및 마이크로 세분화를 강화했습니다. 이는 위에서 언급한 보안 탄력성 점수를 30% 향상하기 위해 Zero Trust의 " 성숙한" 구현으로 분류했던 것입니다.



" 결국 Zero Trust는 어떤 기술에도 적용될 수 있는 철학입니다. 기술만으로는 충분하지 않으며 모든 조직의 여정은 각자가 선택한 목적지로 향하는 다양한 경로를 택할 것입니다. 핵심 원칙을 구현하는 데 적합한 기술 조합을 찾는 것이 궁극적으로 더 탄력 있는 비즈니스를 위해 Zero Trust 보안의 전체 이점을 활용하는 것입니다."

— Wendy Nather,
시스코 CISO 자문 책임자

6. XDR (Extended Detection and Response) 역량

현대의 사이버 위협이 다양한 벡터를 통해 침투한다는 것은 최신 헤드라인을 훑어보는 것만으로도 충분합니다. 그러나 의심이 들고 더 설득력 있는 설명이 필요하면 MITRE ATT&CK 프레임워크에 나열된 수백 개의 공격 기술(및 하위 기술)에 대해 자세히 알아보실 수 있습니다. 중요한 점은 이러한 요령과 기술을 모두 효과적으로 탐지하고 대응하기 위해서는 유리한 고지를 다수 확보해야 한다는 것입니다.

XDR(Extended Detection and Response)은 네트워크, 클라우드, 엔드포인트, 애플리케이션에서 데이터를 시각화하면서 분석 및 자동화를 적용하여 현재와 미래의 위협을 탐지, 분석, 추적 및 해결합니다. 아마 이 기능이 향하는 방향을 짐작하실 수 있을 것입니다. 탐지 및 대응 기능이 더 많은 위협 벡터와 엔터프라이즈 자산을 포함하도록 확장됨에 따라 보안 탄력성이 크게 향상되었을까요? 지금부터 알아보겠습니다.

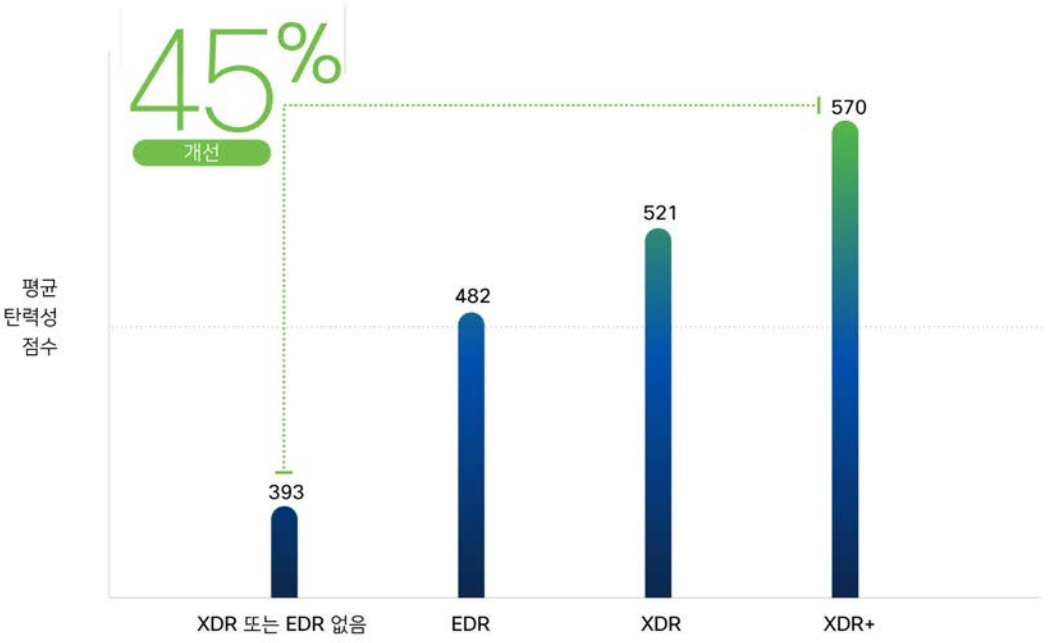
±45% 성숙한 XDR이 구현되지 않은 조직과 구현된 조직 간의 평균 탄력성 점수 차이

이를 테스트하기 위해 XDR 또는 이전에 사용한 엔드포인트 탐지 및 대응(EDR)에서 진보가 없었던 조직을 위한 기준을 수립하겠습니다. 이러한 조직의 보안 탄력성 평균 점수는 393점입니다. 이 점수는 모든 참가자의 보안 탄력성 중 14 백분위수에 해당합니다. 분명 대부분이 피하고 싶어하는 수준입니다.

많은 사람들이 EDR을 XDR의 기본 구성 요소로 보기 때문에, 이를 해당 여정에서의 1순위 마일스톤으로 보겠습니다. EDR을 롤아웃한 조직은 전체 보안 탄력성 점수가 기준보다 23% 증가했습니다. 결코 나쁘다고 할 수 없습니다. 하지만 XDR은 아니니 계속 진행하겠습니다.

XDR의 기본 요소를 갖추고 있는 참가자는 보안 탄력성 점수에 10% 포인트를 추가하여 해당 점수가 EDR 또는 XDR을 구축하지 않은 조직보다 33% 더 높습니다. " 기본" 이란 엔드포인트와 네트워크에서 탐지 및 응답 기능을 갖추고 있지만 아직 모두 통합하지는 않았다는 뜻입니다.

그림 16: XDR 구현 마일스톤이 보안 탄력성에 미치는 영향



출처: 시스코 보안성과연구

기능을 확장하는 것은 좋지만, 보안 운영 분야에서 일한 적이 있다면 누구나 더 광범위하고 깊은 가시성으로 인해 발생하는 과제를 잘 알고 있습니다. 분류과 대응이 필요한 이벤트의 양이 계속 증가할 때 헤드라인에서 읽었던 많은 보안 사고가 발생하는 것입니다. 우리는 XDR의 기본 구성 요소를 응집력 있는 솔루션으로 통합하는 두 가지 주요 요소가 있다고 생각하는데, 이는 사이버 위협 인텔리전스와 자동화/조정입니다.

탐지 및 응답 기능은 찾아야 할 대상과 찾을 방법을 알고 있을 때 가장 효율적으로 작동합니다. 이를 위해 양질의 사이버 위협 정보를 기대하는 사람들이 많습니다. 보안 자동화 및 오케스트레이션은 성숙한 XDR 구현의 결합 조직입니다. 이 기능들이 함께 작동할 때 XDR을 한 단계 개선합니다. 이러한 기능을 모두 갖춘 조직은 9개의 탄력성 성과 전체에서 크게 개선되었으며 XDR에 대한 진전이 없는 조직보다 전체 탄력성 점수가 45% 더 높았습니다.

7. 보안을 엣지에 배치

모바일 인력, 디바이스 확산, 여러 클라우드 공급업체를 통한 애플리케이션 하이퍼 분산을 비롯한 하이브리드 작업의 가속화로 인해 인간의 규모를 능가하는 광범위한 상호 연결성 보안에 대한 과제가 증가하고 있습니다. 현재 널리 사용되는 보안 연결 모델은 이러한 문제를 해결하기에 역부족입니다. 따라서 엔드 유저와 IT 전문가 모두 경험이 파편화되고 노출되는 현실에 직면하게 됩니다.

보안 액세스 서비스 엣지(SASE)는 네트워킹 및 보안을 클라우드 제공 서비스에 통합하고, 운영을 간소화하며, 끊임없이 변화하는 비즈니스 요구에도 탄력성을 유지하는 전략을 제공합니다. 본 보고서를 통해 SASE가 정말로 탄력성 향상과 상관관계가 있다는 증거를 확인할 수 있었을까요? 네, 그렇습니다!

±27% 성숙한 SASE를 구현하지 않은 조직과 구현한 조직 간의 평균 탄력성 점수 차이

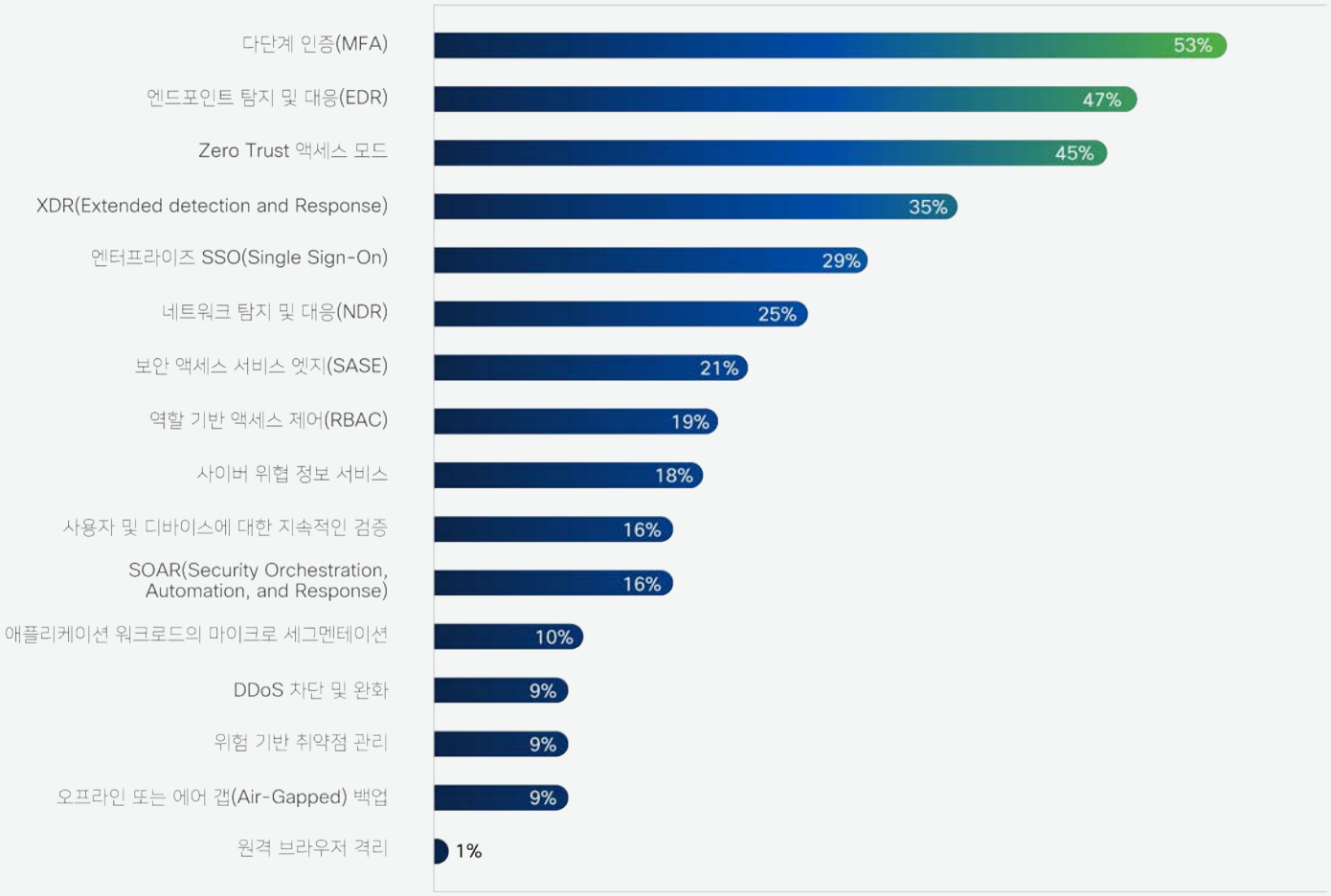
여기서 SASE 구현의 기존 구성 요소(Gartner의 정의 참조)는 구체적으로 다루지 않았지만, 해당 방향으로 향하는 참가자들의 전반적인 진행 상황에 대해 질문했습니다. SASE를 구축했다고 주장하는 조직은 SASE 관련 계획이나 진전이 없는 조직보다 평균 15% 더 높은 전체 보안 탄력성 점수를 보입니다. 또한 SASE 구현이 9개의 개별 보안 탄력성 성과 중 8가지가 훨씬 더 큰 성공 비율을 보여주는 것과 관련이 있다는 점을 발견했습니다.

하지만 이게 다가 아닙니다! 시스코는 Gartner의 SASE 정의를 확장하여 다른 구성 요소 중에서도 고급 위협 탐지 및 대응 기능을 포함합니다. 우리는 이러한 기능에 대해 질문을 던진 후에 SASE 구현과 이러한 기능을 통합한 조직의 탄력성이 더 강한지 궁금했습니다. 해당 조직은 실제로 새로운 수준의 보안 탄력성을 갖추어 SASE를 구축하기 시작하지 않은 조직의 기준보다 27% 더 높은 점수를 받았습니다.

일부 이니셔티브 표시

우리는 이 대규모 설문조사와 함께 IT 및 보안 임원진으로 구성된 포커스 그룹에 조직의 사이버 탄력성 향상을 위한 현재 주요 이니셔티브 3가지를 공유할 것을 요청했습니다. 그 대답은 다음과 같습니다.

그림 17: 보안 탄력성을 위한 주요 이니셔티브



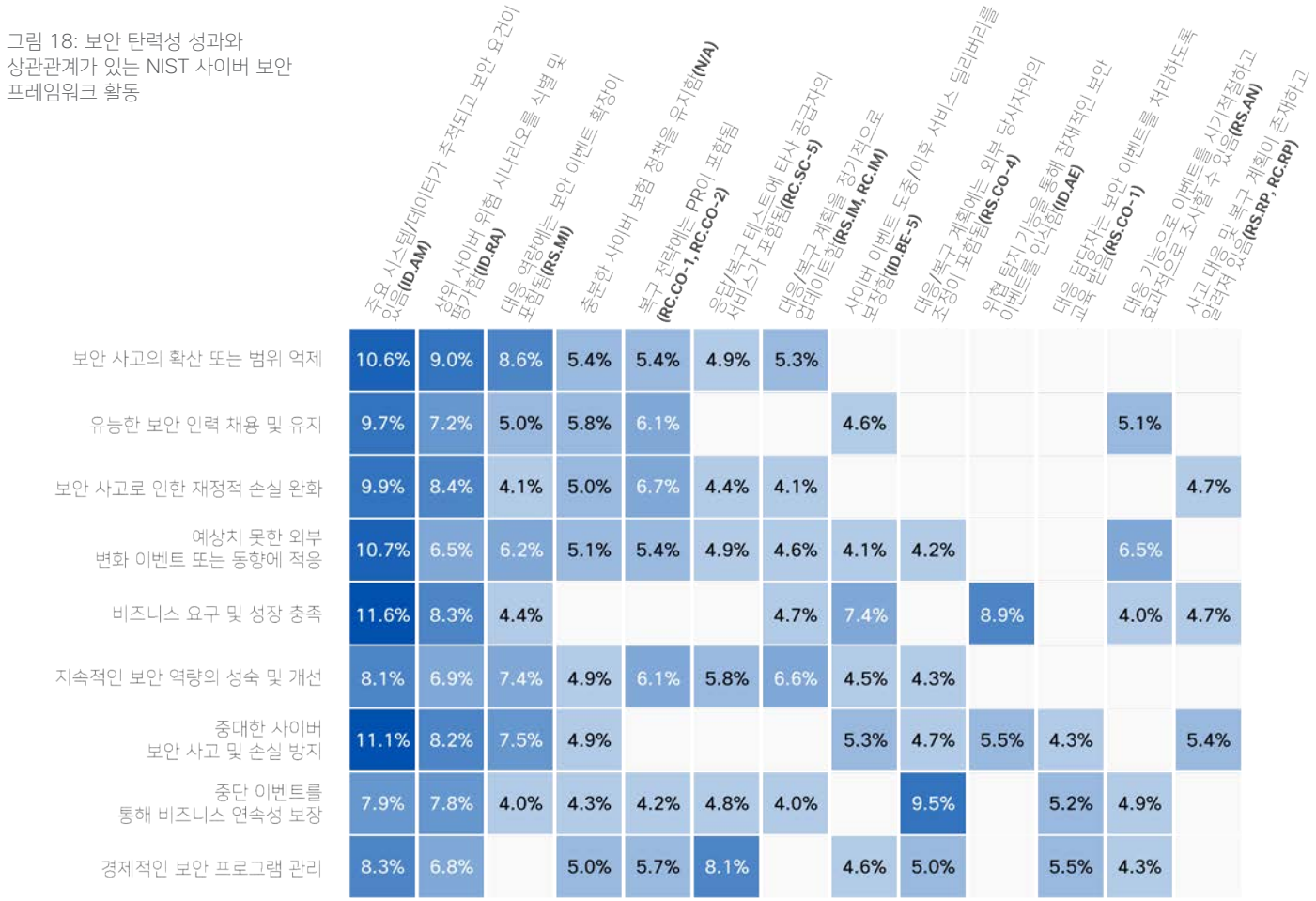
출처: 시스코 보안성과연구

사이버 보안(탄력성) 프레임워크

원래 중요한 인프라 보안을 목표로 한 2013년 미국 행정 명령의 성과였던 NIST 사이버 보안 프레임워크는 사이버 위험을 최소화하고 탄력성을 강화하기 위해 현재 전 세계의 다양한 수많은 조직에서 사용되고 있습니다. 그러한 광범위한 사용으로 인해 사이버 보안 프레임워크에 정의된 관련 활동이 9가지 보안 탄력성 성과에 어떤 영향을 미치는지 평가하는 것이 유용하리라고 판단했습니다.

이 목적을 위해 각 참가자들에게 사이버 보안 프레임워크에 정의된 활동에서 파생된 13개 기능의 하위 집합에 대한 구현 수준을 평가해 달라고 요청했습니다. 이러한 기능은 보안 탄력성과의 잠재적 관련성을 기반으로 시스코 전문가들이 선택했습니다. 그런 다음 각 기능과 보안 탄력성 성과 간의 상관관계를 확인하기 위해 데이터를 분석했습니다. 그 성과는 아래의 효과 매트릭스에 나와 있습니다.

그림 18: 보안 탄력성 성과와 상관관계가 있는 NIST 사이버 보안 프레임워크 활동



출처: 시스코 보안성과연구

파란색 사각형은 NIST 기능과 보안 탄력성 성과가 통계적으로 유의한 상관관계가 있음을 의미합니다. 파란색 사각형 안에 있는 백분율은 해당 기능을 가장 효과적으로 구현한 조직에서 해당 성과를 성공적으로 달성할 가능성이 증가했음을 나타냅니다. 즉, 주요 시스템과 데이터를 제대로 추적하는 참가자는 보안 사고의 확산 및 범위(왼쪽 상단 사각형)를 억제하는 데 약 11% 더 뛰어납니다. 다른 모든 항목도 동일한 방식으로 해석할 수 있습니다.

이 시리즈의 1권에 대한 원래 보안 성과 매트릭스와 마찬가지로, 이 차트는 마치 모험을 선택하는 게임과 같습니다. 특정 탄력성 성과를 개선하는 방법을 알고 싶은 경우, 왼쪽에서 하나를 선택한 후 이를 달성하기 위한 데이터 백업 옵션을 찾으십시오. 반면에 사이버 보안 프레임워크 내의 특정 활동이 조직의 탄력성을 어떻게 강화할 수 있는지 궁금한 경우, 맨 위에 있는 것을 선택하고 교차 성과 목록을 확인하십시오.

우리는 그런 정신에서 매트릭스를 통해 자신의 모험을 선택하여 아래 나열된 관찰 결과를 도출하게 되었습니다. 이러한 사항들 외에도 얼마든지 다른 의견이 가능하니 직접 살펴보십시오. 따라서 우리의 의견을 참고하지 않으려면 바로 결론으로 넘어가십시오.

관찰 1

자신이 무엇을 방어하고 있는지 파악하십시오

맞습니다. " 시스템에 패치만 적용하면 된다" 는 식의 보안에 관련된 상투적인 표현입니다. 그리고 맞습니다. 이 개념은 수많은 PowerPoint 슬라이드가 " 중요 자산 보호" 에 대한 언급과 손자(孫子)의 인용문으로 채워졌습니다. 하지만 그런 행동에는 정당한 이유가 있을 수도 있습니다.

여기서 데이터의 메시지를 무시하기는 어렵습니다. 주요 시스템 및 데이터 추적은 전체 활동 중 가장 효과가 있는 1위 항목입니다. 상위 사이버 위험 시나리오 식별은 2위입니다. 즉, NIST 사이버 보안 프레임워크 식별 기능에 속하는 두 가지 활동이 탐지, 반응, 복구와 같은 일반 탄력성과 관련된 기능보다 보안 탄력성을 향상하는 데 더 많은 역할을 할 수 있습니다. 생각(그리고 행동)할 거리가 되지 않습니까?

관찰 2

사이버 탄력성은 개인만의 문제가 아닙니다

탄력성 성과와 관련 사이버 보안 프레임워크 활동을 살펴보면, 조직의 성공 중 상당 부분이 외부 당사자와 관련이 있다는 느낌을 무시하기 어렵습니다. 충분한 사이버 보험으로 방어를 뒷받침하는 것은 전체 4위입니다. 사고 대응 및 복구 프로세스 중 PR 관리는 5위입니다. 6위는 필요한 타사 서비스 테스트이며, 8위는 해당 서비스가 사이버 이벤트 중에도 계속 제공되도록 보장하는 것입니다. 마지막으로, 외부 당사자들과의 대응 계획 조정이 9위입니다.

따라서 우선순위에 맞는 준비로 예기치 않은 파괴적인 사이버 이벤트에 대비하십시오. 하지만 그날이 오면 혼자 대처하지 마십시오. 실제 경험과 이 데이터는 사이버 탄력성의 실제 범위가 여러분 자신의 경계와 사람을 훨씬 넘어선다는 것을 분명히 보여줍니다.

관찰 3

사람 및 계획의 높은 ROI

마지막 포인트 끝의 사람에 대한 언급은 위 매트릭스의 또 다른 주제로 이어집니다. 즉, 다수의 사이버 보안 프레임워크 활동은 사람 또는 (사람을 염두에 두고 만들어진) 계획을 포함합니다.

하나의 활동은 사고 대응 계획을 수립하고 직원에게 전달합니다. 또 다른 활동에서는 가만히 있기보다는 정기적으로 계획을 업데이트하기를 요구합니다. 그리고 외부 당사자와의 조정을 포함하는 대응 계획의 중요성은 이미 언급했습니다. 물론, 대응 직원이 이러한 계획 수행 방법에 대해 적절한 훈련을 받지 못하면 어떤 계획도 소용이 없습니다.

조직이 보안 탄력성을 향상할 수 있게 지원하는 기술 솔루션은 많습니다. 그러나 이러한 각 솔루션에는 사이버 위기 중에 솔루션을 구성하고 유지 및 운영하는 사람들이 있습니다. 조직이 해야할 일과 그 방법을 알 수 있게 지원하십시오.

관찰 4

돈이 전부는 아니지만...

...보안 이벤트로 인한 재정 손실을 완화하는 것은 과거에 큰 사고를 겪은 CISO와 조직에 가장 중요한 탄력성 성과입니다. 따라서 우리가 분석한 바에 따르면 13개의 사이버 보안 프레임워크 활동 중 8개가 해당 성과를 달성할 가능성을 높인다는 점을 알 수 있습니다.

이러한 활동은 모두 나열하지 않겠습니다. 직접 목록을 만든 다음 NIST 문서를 참조하면 추가 정보와 구현 지침을 확인하실 수 있습니다. 우리가 할 일은 매트릭스에서 강조된 효과적인 활동이 거버넌스, 사람, 프로세스 및 기술 기반 제어에 걸쳐 있음을 강조하는 것입니다. 이는 손실을 최소화하고 탄력성을 극대화하려면 1차원 포인트 솔루션을 훨씬 뛰어넘는 것이 필요하다는 주제를 입증합니다.

결론

자, 이제 탄력성이 좀 개선된 것 같으신가요? 아니면 적어도 탄력성으로 향하는 길에 들어선 것 같다고 생각하시나요? 보안 탄력성을 구축하려면 많은 노력이 필요하지만, 그 시작은 계획입니다.

앞으로 어떤 일이 있더라도 번창할 수 있도록 조직을 구성하실 때 시스코는 해당 계획을 개발하고 실행하며 혼란 속에서도 확실한 방법을 찾으실 수 있게 지원할 준비가 되어 있습니다. 위험 평가, 랜섬웨어, 규정 준수, 대응 및 복구 또는 기타 보안 문제로 고군분투 중이시던 그렇지 않던, 홀로 하실 필요는 없습니다.

추가 정보:

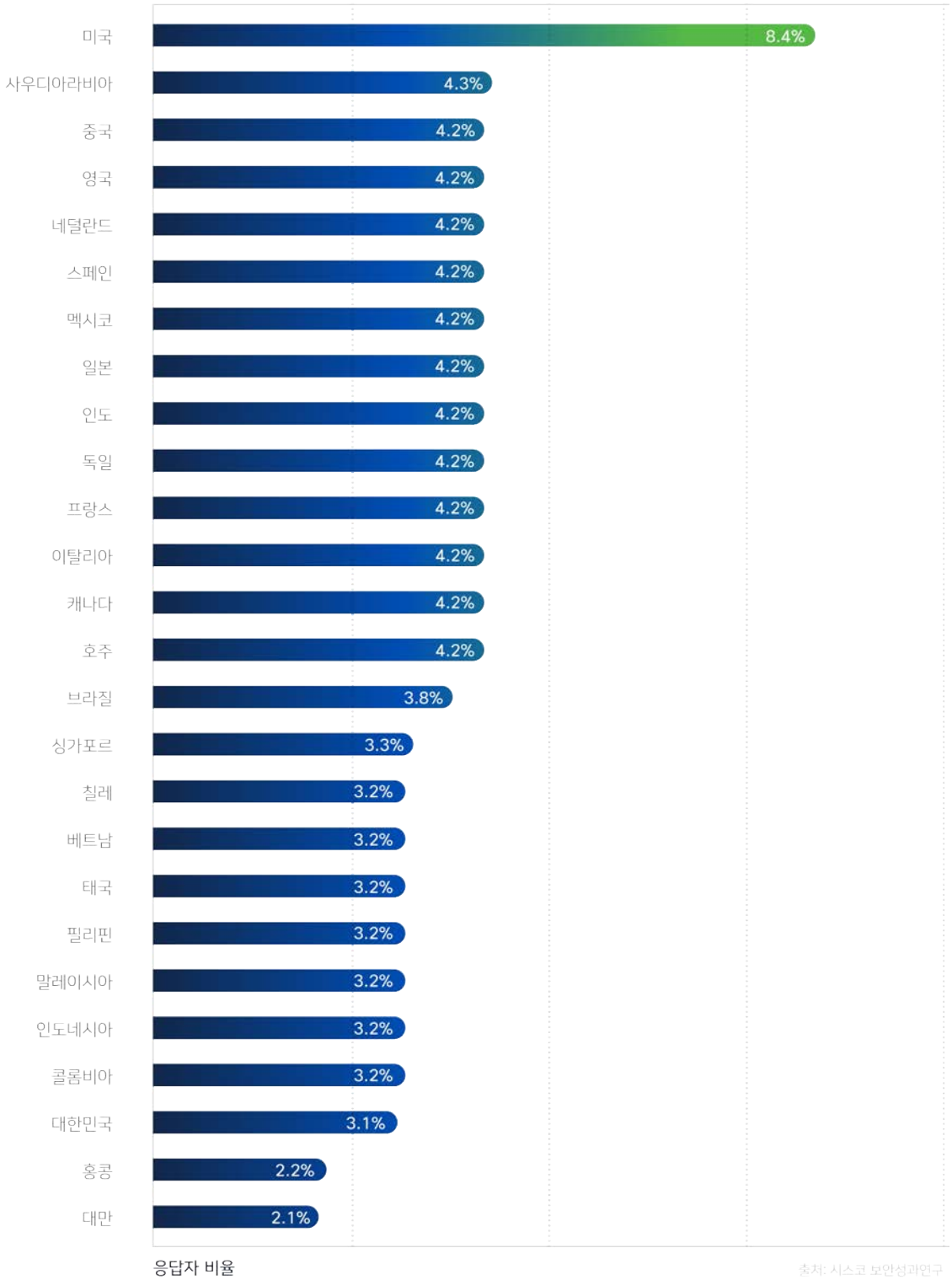
- 시스코의 데이터 중심, 연구 기반 자료 살펴보기
- 보안 탄력성으로 비즈니스를 보호하는 방법 자세히 알아보기

Cisco Secure 소개

오직 최고의 보안을 추구한다는 원칙으로 탄생한 Cisco Secure는 고객 중심의 합리적인 보안 방식으로 구축, 관리 및 사용이 간편할 뿐 아니라 모든 기능이 서로 연동되면서 시너지 효과를 발휘합니다. 가장 광범위하고 가장 통합된 플랫폼을 통해 위치에 상관없이 Fortune 100대 기업 전부의 보안을 책임지고 있습니다. 간소한 보안 환경에서 성공을 앞당기고 미래를 보장받는 방법을 자세히 알아보려면 cisco.com/go/secure를 참조하십시오.

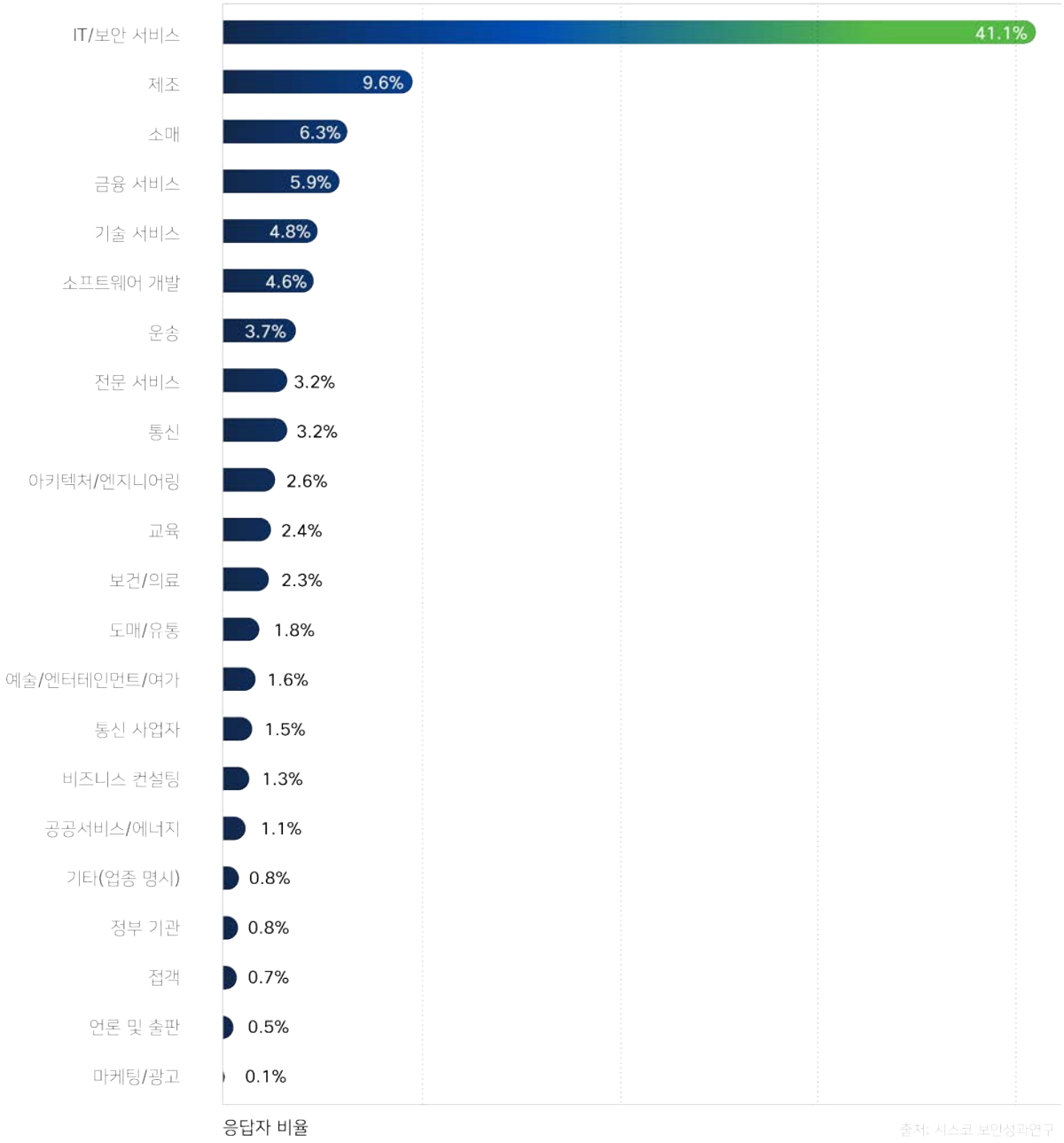
부록 A:
참가자 인구통계

그림 A1: 참가자들이 주로 영업하는 시장



출처: 시스코 보안성과연구

그림 A2: 참가 조직의 대표 산업



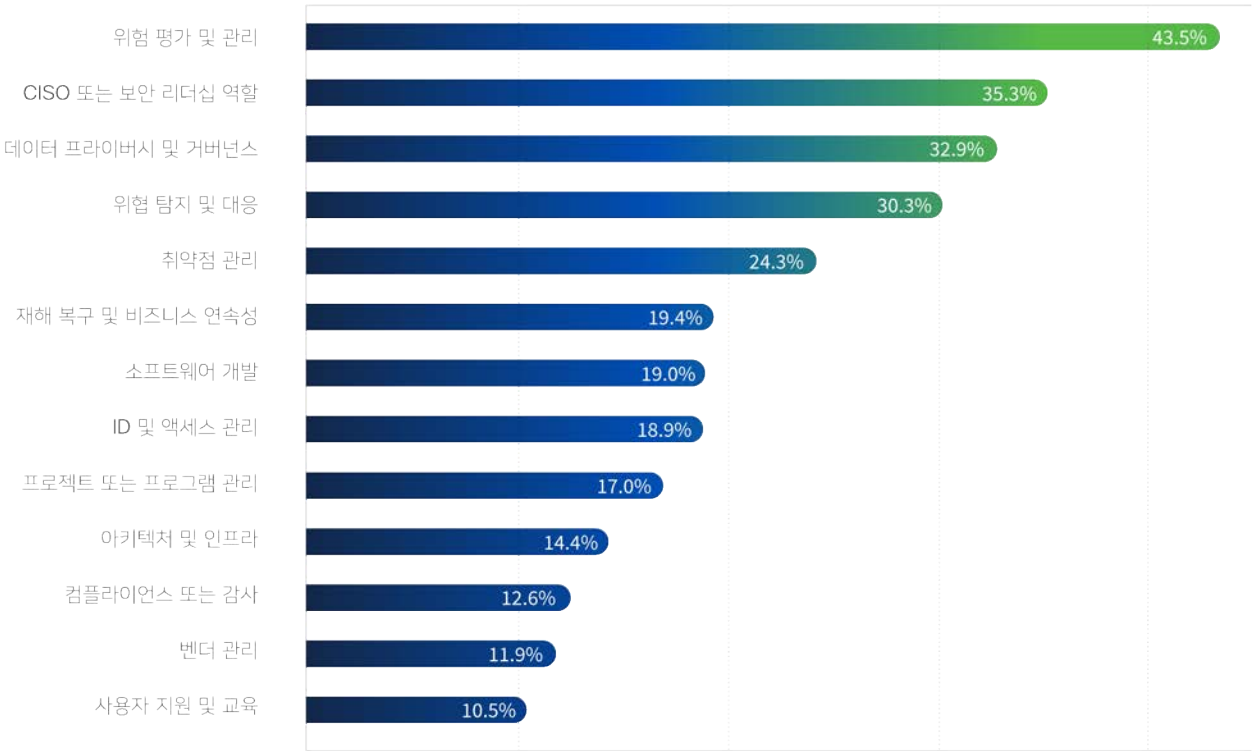
출처: 시스코 보안성과연구

그림 A3: 참가 조직의 직원 수

응답자 비율

출처: 시스코 보안성과연구

그림 A4: 응답자의 기본 보안 역할과 책임



응답자 비율

출처: 시스코 보안성과연구

부록 B:
보안 탄력성 성과

1. **보안 사고의 확산 또는 범위 억제:** 보안 사고가 발생하면, 그 범위는 수평 이동, 권한 상승, 유지 시간, 다른 부서로의 전파 등을 제한하는 제어와 프로세스에 의해 억제됩니다. 훨씬 더 컸을 수도 있는 사고를 억제하거나 이러한 기능을 검증하는 최근의 테스트를 점검한 기록이 여기서 성공의 지표가 될 것입니다.

2. **보안 사고로 인한 재정 손실 완화:** 보안 사고가 발생하면 영향 범위와 관련 손실을 완화하는 제어 및 프로세스를 통해 비용을 절감합니다. 예로는 빠른 복구, 브랜드 피해 제한, 다른 당사자들에 대한 다운스트림 손실 감소, 소송 회피, 사이버 보험을 통한 이전 위험 등을 위한 계획과 절차를 들 수 있습니다. 최선을 바라거나 " 앞으로 닥칠 일에 대처하겠다" 는 전략은 어려움을 겪는다는 징후일 것입니다.

3. **예기치 않은 외부 변화 이벤트 또는 동향에 적응:** 보안 프로그램은 민첩하며 조직 외부에서 예측할 수 없고 통제할 수 없는 이벤트로 변화하는 상황에 효과적으로 대응할 수 있습니다. 코로나19 팬데믹 중 갑작스러운 원격 인력 전환에 잘 적응하고 하이브리드 업무의 후속 동향을 처리하며 디지털 전환을 가속화하는 것은 성공의 증거가 될 것입니다.

4. **비즈니스 요구 및 성장에 발맞춤:** 보안 프로그램이 변화하는 비즈니스 요구에 잘 대응하고 신규 수익 창출을 방해하지 않습니다. 경우에 따라 보안이 경쟁 우위를 제공하거나 순수익을 창출할 수도 있습니다. 비즈니스 임원진이 보안을 비즈니스 장애물로 간주하거나 순전히 비용 센터로 간주한다면, 이는 이 목표를 달성하기 위해 고군분투하고 있다는 신호입니다.

5. **보안 기능의 지속적인 성숙 및 개선:** 보안 프로그램은 목표를 설정하고, 진행 상황을 추적하며, 시간 경과에 따른 지속적인 효율성 개선을 추구합니다. 이 프로그램은 아직 모든 영역에서 성숙하지 않을 수 있지만, 가장 개선해야 할 부분이 무엇인지 알고 이에 대한 계획을 수립해야 합니다. 최신 위협에 뒤처지는 정체된 보안 프로그램이나 다음 제어 기능 시행 후 " 완성" 되는 철학은 어려움을 겪는다는 신호일 것입니다.

6. **주요 사이버 보안 사고 및 손실 방지:** 이 목표를 성공적으로 달성한 조직에서는 지난 몇 년간 심각하거나 영향이 큰 보안 사고(높은 내/외부 가시성)가 발생하지 않았을 것으로 추정됩니다. 또한 중대 손실 사고가 발생하는 것은 시간 문제일 뿐이라고 의심할 이유가 없습니다. 경미하거나 중등도의 사고가 예상되지만, 언론에 보안 사고가 실리지 않을 정도로 지속적인 보안을 유지합니다.

7. **중단 이벤트를 통해 비즈니스 연속성 보장:** 시스템 장애, 네트워크 중단 및 기타 기술 중단은 중요한 비즈니스 운영에 미치는 영향을 최소화합니다. 조직은 광범위하거나 신속한 아키텍처/프로세스 변경을 강요하는 갑작스럽고 예기치 않은 이벤트를 성공적으로 탐색할 수 있습니다.

8. **비용 효율적인 보안 프로그램 유지:** 임원진은 보안 프로그램의 ROI가 양호한 것으로 봅니다. 높은 보안 비용에 대해 반복적인 불만이 없습니다. 셸프웨어 구매 비율이 낮습니다. 인력이 초과되지도 않지만 아주 부족하지도 않습니다. 경영진과 보안 책임자가 위험을 늘리지 않으면서 보안 예산을 절약하고자 계획한다면 이러한 목표를 성공적으로 달성하고 있다는 신호입니다.

9. **우수한 보안 인력 모집 및 보유:** 조직은 보안 커뮤니티에서 일하기 좋은 직장이라는 긍정적인 평판을 얻고 있습니다. 새로 모집하는 보안 직책은 대개 과도한 인센티브 없이도 신속하게 충원 마감됩니다. 유능한 인재들이 퇴사하지 않고 승진하며, 인력의 자연 감소율이 낮습니다. 직원 만족도가 지속적으로 높습니다.

CISCO
SECURE

미주 본사
Cisco Systems, Inc.
캘리포니아 주 새너제이

아시아 태평양 본사
Cisco Systems(USA), Pte. Ltd.
싱가포르

유럽 본사
Cisco Systems International BV
네덜란드 암스테르담

2022년 발행

cisco The bridge to possible